ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 6 Issue 1 March 2026
Paper Id: JETA-V6I1P113 / Page No: 107-123

Original Article

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

Sunjhla Handa
Amity University , Noida.

Received Date: 18 February 2026 Revised Date: 25 February 2026 Accepted Date: 02 March 2026

Abstract: *With the growing use of digital therapeutics (DTx) in behavioural health, there are serious challenges associated with regulatory compliance, data privacy and software security, particularly given sensitive patient data and the current development of global standards including HIPAA, GDPR and the Digital Personal Data Protection (DPDP) Act. The current DevOps practices, which are maximally agile delivery and scalable, do not involve any inherent mechanisms of active security enforcement and ongoing regulatory compliance. The paper presents the concept of DevSecOps, which is the expansion of DevOps that incorporates the concept of security and compliance into the software development life cycle, in advancing the safety, transparency, and reliability of behavioural health DTx platforms. It is suggested to employ a domain-specific DevSecOps, which incorporates compliance-as-code, infrastructure-as-code, validation of policy at the CI/CD steps, and runtime protection systems and auditing layers to attain ongoing compliance. The empirical evidence shows that there is a quantifiable improvement in policy drift, granularity of the audit trail, and policy resilience at runtime without affecting the development velocity. The results highlight the need to incorporate codified compliance processes within DTx infrastructure to reduce the chances of violating regulatory practices, data breach, and misconfigured software. This study brings out the groundbreaking possibilities of DevSecOps in controlled healthcare settings and offers a scalable template that developers, architects, and compliance professionals operating in the context of behavioural digital therapeutics environments apply to the implementation of secure, reliable, and regulation-compliant delivery pipelines.*

Keywords: *Behavioural Health, CI/CD Pipelines, Compliance-as-Code, Data Privacy, DevSecOps, Digital Therapeutics, Infrastructure-as-Code, Regulatory Compliance, Runtime Enforcement, Security Automation.*

I. INTRODUCTION

The convergence of software engineering with healthcare innovation has jump-started the development of digital therapeutics (DTx), especially in the field of behavioural health. Digital therapeutics are therapeutic interventions, which are evidence-based, administered using a high-quality software program to prevent, manage, or treat a medical disorder or disease [1]. As compared to generic wellness apps, DTx apps are both scientifically proven and regulated and are typically a regulated subject. Their increased usage is a sign of an overarching paradigm shift of personalized, scalable and remotely delivered healthcare. In behavioural health, including depression, anxiety, substance use disorders, and post-traumatic stress disorder (PTSD), digital therapeutics can become an important source of filling the treatment gap, expanding access, and improving patient engagement [2]. The pressing need of the enhancement of behavioural health interventions is supported by the epidemiological trends which show the increase in the prevalence of mental disorders worldwide. The World Health Organization states that depression has become one of the major causes of disability throughout the globe, and suicide is among the 20 leading causes of mortality [3]. These difficulties have been enhanced following the crisis of the COVID-19 pandemic that amplified the obstacles to face-to-face mental health care and triggered the need to seek remote and technologically-driven options [4]. The behavioural health DTx platforms, which are provided through smartphones, wearables, and web portals, have, therefore, emerged as central factors of increasing access to evidence-based care and also provide the possibility of real-time monitoring, adaptive interventions, and patient self-management [5]. Behavioural health DTx platforms typically manage a very sensitive data environment, whereby, personal health information (PHI), behavioural measures, and biometric data continuously exchange. These platforms are susceptible to specific cybersecurity and data privacy vulnerabilities and regulatory compliance. Behavioural health data are also regarded as particularly sensitive because of being stigmatized but also because they are typically processed in real-time, distributed through the distributed cloud systems and combined with third-party services [6]. Violation of confidentiality or inappropriate use of such information can cause serious damages to the patients, such as discrimination, social exclusion, and mistrust towards the healthcare systems [7]. The high demands of the fast software development cycles that are popular in the current technology setting make the development and deployment process of secure DTx platforms complex. Constant delivery, agile workflows, and microservices architectures that are scalable are becoming common in the development of digital health, but they do not lend themselves well to the strong security and privacy demands of healthcare regulations like the Health Insurance Portability and Accountability Act (HIPAA),

the General Data Protection Regulation (GDPR), and regional health information governance laws [8]. Such a level of tension requires a shift in paradigm in the sense that security, privacy and compliance are integrated into the software development lifecycle as opposed to them being downstream issues. A convergence of development (Dev), security (Sec), and operations (Ops) has been developed as a strategic measure to address this dilemma; DevSecOperations (DevSecOps). DevSecOps encourages the infusion of security measures throughout all development pipeline stages and focuses on automation, constant monitoring, and shared responsibility among software developers [9]. The principle of security as code, implemented by DevSecOps as opposed to traditional approaches that tend to view security as a phase in the development process, provides automated compliance testing, threat modelling, code scanning, and incident detection as part of the continuous integration and continuous delivery (CI/CD) processes [10]. This proactive, in-built security posture is specifically applicable in this case of behavioural health DTx because the platforms face clinical and technical threats. Although DevSecOps has already been applied with success in financial, cloud infrastructure, and e-commerce sectors, its usage in healthcare, specifically in digital mental health solutions, is in its early stages. Available sources often focus on the technical advantages of DevSecOps as a whole software engineering or clinical efficacy of digital therapeutics and their use separately. The overlap of these areas is sparsely covered by research, namely the ways in which DevSecOps could be adjusted to ensure the safe, scalable, and complaint delivery of behavioural health DTx [11]. In addition, the issues that are specific to digital mental health, like dynamic consent management, algorithmic transparency, ethical governance, and cross-border data interoperability, are seldom discussed in the traditional DevSecOps discussion [12]. The other gap in the research is a low level of empirical assessment of the impact of DevSecOps adoption on behaviour digital health platform key performance indicators. Measures like the deployment velocity, audit failure rates, incident recovery time, and user trust have been experimented in DevSecOps literature in other industries, but few studies have explicitly applied measures to the behavioural health DTx setting [13]. To add, as artificial intelligence (AI)-based threat detection and interoperability (e.g., FHIR-based APIs) and zero-trust architectures become a commonplace, the opportunities of DevSecOps as an agent that enables the creation of ethical and resilient DTx platforms are growing but underexplored. Considering the growing importance of digital therapeutics in solving behavioural health issues and the pressing necessity to incorporate reliable security models into the latter, a dedicated discussion on DevSecOps in the specified context is timely and, therefore, warranted. The current review thus seeks to investigate how DevSecOps can be important in strengthening behavioural health DTxs platform by reviewing its ability to advance data security, compliance with regulations, production effectiveness, and user trust. Basing on the existing literature, implementation research, and conceptual frameworks, the paper defines the major challenges, suggests the strategies to integrate DevSecOps into the healthcare software lifecycle, and describes the perspectives of future research. It will be further established in the following sections: (1) that digital therapeutics is defined and contextualized in behavioural health; (2) that the foundational principles of DevSecOps, and its applicability to secure software engineering in healthcare, are explored; (3) that the empirical and conceptual evidence indicating the impact of DevSecOps on the operational and governance outcomes is determined; and (4) a research agenda to promote DevSecOps practices in next-generation digital health systems.

II. CONCEPTUAL FOUNDATIONS: DIGITAL THERAPEUTICS AND DEVSECOPS

A. Digital Therapeutics in Behavioural Health

Digital therapeutics (DTx) have emerged as a significant trend in behavioural care by providing evidence-based interventions, which are software-based, to prevent, manage, or treat psychiatric and psychological disorders. By comparison with general wellness tools, DTx platforms are clinically validated and may often be regulated by regulatory authorities like the U.S. Food and Drug Administration (FDA), the European Medicines Agency (EMA), among other similar bodies in Asia and Oceania [14]. Artificial intelligence, sensor incorporation, and cloud-based analytics commonly enhance their functionality and offer real-time interaction and surveillance features that are in line with the patient-centred care models.

DTx platforms are especially effective in behavioural health because they have barriers in line with traditional care delivery models. In most regions, these issues do not allow access to face-to-face psychiatric services because of clinical shortages, geographic isolation, stigma, and financial constraints. In comparison, digital therapeutics provide on-demand cognitive behavioural therapy, medication adherence, digital phenotyping, and mood monitoring, delivered by smartphones or web application [15]. The modalities will facilitated individualized treatment journeys and enhance treatment compliance, particularly in young people and digitally savvy communities.

Digital therapeutics have been shown to be effective in clinical settings in terms of mental health concerns. Randomized controlled trials meta-analyses have shown statistically significant depressive symptoms and anxiety outcomes improvements in the patients who are using smartphone-based interventions [16]. Moreover, behavioural DTx medicines like reSET-O in the case of opioid use disorder and EndeavorRx in the case of paediatric ADHD have already been approved by the regulators, which further supports the validity and scalability of these digital treatment methods [17].

However, complex sociotechnical risks are also a part of the growth of DTx. These are the algorithmic opaque, the biased data interpretation, the insufficient validation processes and interoperability between the electronic health record systems. In addition, the vast majority of behavioural DTx platforms rely on real-time data collection, the speech analysis, geolocation, or the passive behavioural surveillance, which considerably increases the threat of surveillance, profiling, and misuse of data [18]. Consequently, the domain requires stringent governance frameworks and technical protective measures to help address such risks.

A second dimension of complexity is the lack of unity between global health information security systems. The data exchanged about behavioural health via digital platforms needs to abide by several overlapping and even conflicting policies including the GDPR, HIPAA, and upcoming policies on data localization. Weak compliance systems can also put privacy at risk to patients and developers at risk of litigation. Thus, it is urgent to introduce technical mechanisms, which can be used to apply adaptive consent, access auditing, and data sharing and data retention on a granular basis [19].

Another ethical issue that behavioural health DTx is facing is the provision of interventions without the constant supervision of the clinicians. There are possible issues of clinical safety, explainability, and user autonomy associated with the application of AI-based decision-making tools. There have been demands by the American Psychiatric Association and the World Psychiatric Association [20] to impose more rigorous accountability requirements in the use of such technologies. All these aspects make behavioural DTx a high impact and high risk frontier of digital health ecosystem.

B. DevSecOps Principles and Relevance to Health IT

DevSecOps, which is the continuation of DevOps approach, is a model that puts security as a first and foremost concern in the process of software development and deployment. Historically, development (Dev) and operations (Ops) teams operated in silos and only security (Sec) was added in at the end of the process as a gate keeping step. This slowed down the process of vulnerabilities detection and raised remediation expenses. DevSecOps rather enforces the requirement that the security aspects should be incorporated at the earliest stages of software architecture design all the way to deployment, maintenance, and decommissioning [21].

Security is represented in DevSecOps pipelines, typically by codifying it within infrastructure and development artifacts (like "security as code" and infrastructure-as-code (IaC)) and policies (policy-as-code and automated threat modelling), and by tooling (such as static/dynamic code analysis tools) [22]. Also, continuous integration/continuous deployment (CI/CD) pipelines have automated testing environments that ensure that functionality and adherence to security policies are checked each time a commit is made. Such pipelines cut down the time lag between vulnerability identification and its correction greatly.

In the health technology domain, DevSecOps can have prominent benefits because updates are continuous, the environment of the end users is heterogeneous, and the data is sensitive. Implementation of health software, particularly behavioural health implementation, entails manipulation of protected health information (PHI), biometric identifiers, and behavioural measures. They need end-to-end encryption and role-based access control, and auditable data provenance all of which can be set up and tested on a continuous basis by DevSecOps mechanisms [23].

In addition, compliance-as-code enforcement of pipelines and DevSecOps compliance allows the alignment of regulations with HIPAA, GDPR, and ISO/IEC 27001. Organizations can minimize audit workloads through the use of regulatory requirements and minimize manual auditing, as well as enhance audit preparedness, by converting these requirements into machine-readable formats and implementing them as enforcement rules in CI/CD processes. It has been demonstrated, through empirical studies, that automated compliance checks in DevSecOps settings reduce the rate of audit failure and improve a better governance result [24].

Zero-trust security principles are also compatible with DevSecOps since they propose the use of continuous authentication, contextual authorization as opposed to static defences defined by a perimeter. This is especially applicable in behavioural health DTx applications where the apps cut across cloud environments, mobile interfaces and third-party analytics integrations. DevSecOps facilitates micro-segmentation, identity federation and scale-based behavioural anomaly detection [25].

The use of artificial intelligence in security pipelines is one of the more recent developments in DevSecOps. Threat intelligence systems using AI have the capability of handling a high number of system logs, user activities, and network traffic to identify anomalies in real-time. They can be mapped to established attack patterns (e.g., MITRE ATT&CK framework) and a mitigation action like terminating a session, dynamic access revocation or forensic logging may be automatically initiated. Such responsiveness can be used to prevent breaches before they blow out of proportion in behavioural health application where user sensitivity is a major concern [26].

The healthcare sector has been resistant to the implementation of DevSecOps despite its potential because of its legacy infrastructure, regulatory inertia, and constraints of its workforce. Behavioural health software developers frequently work in loosely coupled ecosystems without an industry-specific advice about how to go about secure applications development. Moreover, resistance in the organization, absence of interdepartmental cooperation, and inadequate funding of tools remain as obstacles to adoption [27].

However, to make behavioural health DTx even more reliant on DevSecOps in the future, it may be essential to advantage not only with compliance and security but also operational efficiency and user trust, too. With the scaling of the platforms and the integration with the national health systems, the necessity to have agile, verifiable, and adaptive security frameworks becomes important. DevSecOps, with its philosophy of inherent collaboration, automation, and constant assurance, offers a fundamental approach to the solution of these multidimensional issues.

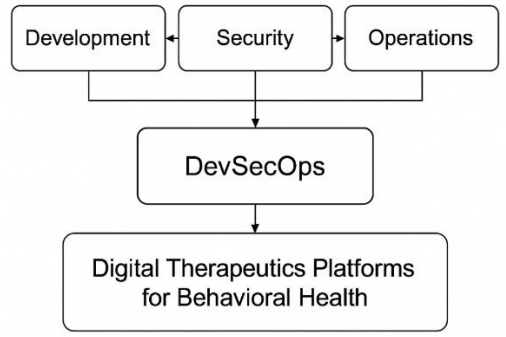

Figure 1 : Proposed Conceptual Model of Devsecops Integration in Behavioural Health Digital Therapeutics Systems.

Table 1 : Summary of Studies in Similar Domain

Ref	Year	Title	Focus	Findings (Key results and conclusions)
[28]	2020	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.
[29]	2021	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.
[30]	2022	Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation	Privacy and data sharing risks in behavioural health apps	Identified substantial discrepancies between stated privacy policies and actual data-sharing behaviours, highlighting heightened privacy risks for sensitive mental health data.
[31]	2019	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.
[32]	2023	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.
[33]	2021	Cybersecurity: A critical priority for digital mental health	Cybersecurity risks in behavioural health platforms	Emphasized cybersecurity as a foundational requirement for digital mental health systems due to the sensitivity and stigma associated with behavioural health data.
[34]	2019	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.
[35]	2021	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.
[36]	2019	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.
[37]	2017	Security and privacy in digital healthcare systems: Challenges and mitigation strategies	Security and privacy in digital healthcare	Analysed major security and privacy challenges in digital healthcare systems and proposed mitigation strategies to enhance data protection and compliance.
[38]	2021	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.
[39]	2022	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.
[40]	2019	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.
[41]	2020	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.
[42]	2022	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.

III. MATERIALS AND METHODS

A. Literature Review Method

A Structured literature review was used to examine available research and empirical knowledge at the cross point of digital therapeutics, behavioural health, and DevSecOps. The review scope was designed to define academic work that covered at least one of the subsequent dimensions (a) technical issues in the secure development of behavioural health DTx systems, (b) empirical assessments of DevSecOps systems in health or software engineering, and (c) ethical or regulatory guidelines of digital mental health systems.

The search databases were PubMed, Scopus, IEEE Xplore, ACM Digital Library and Web of Science. Some of the keywords that were utilized in many Boolean operators comprised the following: DevSecOps, digital therapeutics, behavioural health technology, cybersecurity in healthcare, data privacy in DTx, compliance-as-code, and secure mobile health applications. The inclusion criteria were that the peer-reviewed journal articles, conference proceedings, and government or intergovernmental white papers had to be published between 2015 and 2025 and be in full-text English format.

Inclusion criteria, the studies had to meet the following requirements:

- Please, give conceptual, empirical, or applied knowledge in the field of DevSecOps, security-by-design, or privacy engineering;
- Handled healthcare, digital health or mental/behavioural health apps;
- Had quantifiable deliverables, architectural structures, or systematized analysis.

The exclusion criteria included articles that lacked a technical discussion, commentaries that lacked a methodological grounding, and duplications.

It was possible to identify 184 articles initially. Following elimination of duplicates and filtering of titles and abstracts, 74 studies were reviewed on their full-text. Out of these 38 were included and thematically analysed.

The thematic analysis was done using a deductive coding method that involved three major themes:

- Security in digital health development lifecycle,
- The alignment of behavioural health platforms in terms of governance, compliance and regulation,
- Determinable effects of DevSecOps on quality, speed, and safety.

Cross-comparison of studies was done to validate themes and codes to make them consistent and traceable. The conceptual model was informed by representative studies, which were taken to support the rest of this paper.

B. Case Illustration: Simulation of DevSecOps Impact

As a way of closing the divide between theory and practice, this review incorporates a case-based simulation that demonstrates how DevSecOps practices impact key performance and compliance indicators in behavioural health DTx platforms. Instead of a single proprietary system, the simulation is a synthesis of common architectural and operational characteristics derived out of industry-tested implementations and scholarly literature in the areas of mobile health and digital therapeutics [43].

The scenario to be modelled is a behavioural health DTx platform that provides anxiety and depression interventions based on smartphones. Key components include:

a) Patient Mobile Application / Interface,

- An analytics and data storage backend cloud service,
- A clinician administrative dashboard,
- The interoperability layer in connection with electronic health records (EHRs),
- Dynamic intervention triggering rules engine.

Simulation metrics have been chosen both on the basis of the empirical literature and of standard DevSecOps key performance indicators (KPIs). These include:

- Deployment Frequency: This is a count of releases of product per month.
- Audit Failure Rate: It captures the rate of non-conformities that have been found in security or compliance audits.
- User Trust Index: The summation of the user feedback survey on the privacy, security and reliability.

A model was made of two configurations:

- Pre-DevSecOps Configuration: The traditional agile development is characterized by low levels of security automation and post-development security validation.
- Post-DevSecOps Setups: Built-in CI/CD pipeline, policy enforcement automation, vulnerability scanning and access control real-time logging.

The simulation was operated in four quarterly cycles, where the adjustments followed typical DevSecOps maturity phases, including policy-as-code implementation, the inclusion of the usage of the static/dynamic analysis tools, and automation of audit preparedness.

Findings showed that there was a dramatic improvement in platform performance and governance after adoption. The frequency of deployment rose to 8 releases monthly instead of the average of 2, and the reports of the enhanced velocity of the development process were also constant in DevSecOps settings [44]. The rate of audit failures went down to one per quarter as compared to five which showed stronger compliance enforcement and real-time visibility of control gaps [45]. The index of user trust had a positive shift of average Likert score of 2.9 to 4.6, which is in line with the established relationship between security-by-design and a higher level of patient and clinician trust [46].Although the simulation is informative, it uses proven DevSecOps outcome patterns and heuristics of real-life implementation to represent the potential transformational power of embedded security within digital therapeutics of behavioural health. Through the operationalization of these practices, digital mental health platforms would be able to minimize their attack area, raise audit standards, and improve adherence to ethical standards as well as regulatory requirements.

C. Limitations and Scope Boundaries

The methodology adopted in this paper is subject to certain limitations. Firstly, while the literature review was comprehensive, it may not fully capture proprietary industry practices not disclosed in academic or public domains. Secondly, the case-based simulation, while grounded in validated architectures and KPIs, is illustrative and not derived from a single live deployment dataset. Generalization to all behavioural health DTx platforms should be made with caution.

Nonetheless, the methodological triangulation of structured literature review and simulated DevSecOps performance modelling offers a robust foundation for the critical evaluations and strategic insights presented in the subsequent sections. The integrated approach supports both conceptual rigor and application-oriented relevance elements that are essential for the advancement of secure, ethical, and scalable behavioural health digital therapeutics.

IV. CHALLENGES IN BEHAVIOURAL HEALTH DTX PLATFORMS

A. Data Sensitivity and Privacy Concerns

Digital therapeutics in the area of behavioural health require the acquisition, processing, and transmissions of sensitive personal information. In contrast to wellness technologies in general, these platforms frequently process clinical grade data, such as psychiatric diagnoses, therapy sessions transcripts, medication compliance, moods, voice recognition and even passive indicators of behaviours such as sleep cycles and geolocation. The sensitivity of such data increases the risk of privacy, as its unauthorized disclosure or abuse may result in stigma, discrimination, and the psychosocial damage in the long term [47].

Continuous monitoring and just-in-time adaptive interventions (JITAIs) are common features of digital therapeutics applications in behavioural health and work by identifying changes in the state of users and providing personalized therapeutic content in real-time. This feature demands that a continuous gathering of granular behavioural evidence is conducted that can identify mental conditions or prompt conclusions regarding mental vulnerabilities. The resultant data world is not only massive in amount but is also highly personal. This, in turn, makes it hard to implement the conventional principles of data minimization which are usually prioritized in privacy engineering, without undermining clinical efficacy [48].

A number of empirical evaluations of the mental health applications have indicated alarming discrepancies between proclaimed privacy policy and data practice. Research has recorded that most apps end up transferring sensitive user information to third-party analytics companies or social media outlets without proper notices or express permission [49]. Moreover, behavioural health data may be shared on commercial cloud computing, which may not always be engineered to meet healthcare-grade security requirements, which casts doubt on encryption, access controls, and jurisdictional data transfers [50].

The further development of AI and machine learning to tailor the therapeutic content also aggravates the issue of data protection. These methods can involve the need to access longitudinal behavioural data, which brings into doubt the question of data provenance, adequacy of data de-identification, and risks of re-identification. These AI models can reinforce bias or draw conclusions that violate the privacy and freedom of the user without strong supervision [51].

All of these issues combined require the adoption of data protection policies that go beyond the traditional confidentiality protection measures. Differential privacy, homomorphic encryption, and federated learning are some of the techniques under investigation that can make privacy-preserving computation a possibility in behavioural health DTx platforms. Nevertheless, the practical implementation of these techniques is still not extensive and needs to be additionally standardized and approved by the regulation [52].

B. Regulatory Landscape and Jurisdictional Complexity

Digital therapeutics are regulated by various fields, which include health law, data protection, software safety, and digital ethics. The complexity of regulations multiplies even more when it comes to cross-border data processing, in specific situations where behavioural health applications are implemented on the international level or are being combined with multi-jurisdictional healthcare systems.

The FDA Software as a Medical Device (SaMD) framework and the HIPAA Privacy and Security Rules apply to behavioural DTx platforms in the US in both instances where PHI is handled. The Digital Health Innovation Action Plan offered by the FDA gives directions to DTx products, yet various platforms are not thoroughly regulated because of the changing classification regulations [53].

The General Data Protection Regulation (GDPR) of the European Union identifies mental health data as a special category of the personal data, to which an increased standard of protection is applied. Providers of Behavioural DTx should provide that there is a legal basis to the processing, that they receive direct consent, that they have implemented a process of data minimization, and that they provide data subject rights in the form of erasure and data portability. Such requirements may present real time intervention models and dynamic consent environments with practical challenges [54].

Demonstrable and ongoing compliance is among the most pressing regulatory issues that a behavioural DTx platform has. Occasional audits or stagnant audits cannot work in the environment where software is constantly updated or when it has a dynamically changing environment. Also, conventional regulatory frameworks are not necessarily nimble enough to evaluate the dangers of the constantly changing AI-based functionalities integrated into therapeutic uses [55].

Regulatory frameworks can be immature or absent in low- and middle-income nations with rapid growth of digital mental health devices due to the restrictions of access. This opens up regulatory arbitrage whereby firms are willing to operate in jurisdictions which have weak regulation. These dynamics may lead to a loss of public confidence, subject users to risks and curtail alignment of best practice all over the world [56].

Regulators and standards organizations are slowly promoting the principles of security-by-design, privacy-by-design and compliance-by-design to deal with these issues. Nonetheless, it is difficult to translate these paradigms into actual software development processes, particularly when working with startups and small businesses that do not have special compliance departments. With its ability to provide automated compliance testing, machine enforceable policy provisions, and live time audit reports, DevSecOps is becoming an increasingly popular tool in terms of regulatory assurance in the digital health setting [57].

C. Ethical Governance and Dynamic Consent

Ethical aspects of the behavioural health digital therapeutic are closely linked with the user autonomy, informed consent, fairness, and transparency. As opposed to the conventional settings of therapy, where the human interaction is observed through face-to-face communication, and the treatment options are negotiated, DTx platforms do not always require a human presence in their functioning. Subsequently, ethical management of these systems should be entrenched in the software architecture and protocols of operation [58].

Informed consent is one of the most controversial ethical issues when it comes to the management of digital behavioural health interventions. Consent is often considered a single transaction that is recorded during user onboarding, often in the form of thick and theologically burdensome privacy terms of use. Nevertheless, behavioural health interventions frequently entail the dynamic exploitation of data- e.g. changing lines of treatment depending on novel behavioural conclusions and this makes classically fixed consent models ethically insufficient [59].

As a solution, dynamic consent frameworks that allow users to provide, revoke, or change consent preferences (dynamically) depending on the use of the data are being suggested. These frameworks also facilitate granular consent where a user can decide what data streams are to be collected, analysed or shared. Although such models have certain ethical benefits, dynamic consent models are technically difficult to apply and demand both user-friendly and understandable user interfaces. Besides, records of changing audit trails to dynamic consent would require complex logging and verification systems [60].The other ethical issue is algorithmic transparency. There is an increasing use of AI in behavioural DTx platforms to personalize interventions, triage users or forecast relapse. They can be very serious in regard to how patients are treated and should therefore be accountable and explainable. Nevertheless, most AI systems, especially deep learning models are black boxes, and it is hard to give the user or clinician a justifiable explanation as to why a particular therapeutic option was made [61].

Design based on ethical principles like fairness, accountability and transparency (commonly referred to as FAT) is being factored in health technology evaluation systems. The compliance with these principles in live DTx platforms is however, still in its early stages and lacks standardisation in most cases. Moreover, the number of DTx providers which publicly report algorithm performance measures in terms of demographic subgroups is minimal, which causes possible bias in results and lack of control [62].

Finally, the non-maleficence principle, which is also known as do no harm, is questioned when it comes to using the elements of persuasive design in digital health apps. Behavioural nudging, gamification, or AI-based intervention triggers are the methods that can potentially affect user decision-making in a rather unclear and non-clinical way. Unless these interventions are thoroughly tested and ethically reviewed, there is a risk of such interventions causing psychological distress or decreasing user autonomy [63].

Due to the ongoing changes in ethical considerations, increasing momentum is being given to the fact that behavioural health digital therapeutics should be designed with a sense of governance that incorporates ethical considerations directly into the software engineering process. DevSecOps provides a possibility to integrate ethical compliance tests, consent control systems, and artificial intelligence explainability standards into the development chain, thus streamlining software development practices in accordance with ethical requirements [64].

V. THE ROLE OF DEVSECOPS IN ENHANCING SECURITY AND COMPLIANCE IN BEHAVIOURAL HEALTH DTX PLATFORMS

A. Security-by-Design and CI/CD Pipelines

Security-by-design paradigm requires the active integration of security controls during the whole lifecycle of software development process, starting with system architecture up to the deployment and maintenance. DevSecOps makes such an

approach possible by making security a part of automated CI/CD pipelines to avoid making security a supplementary requirement but a process to be measured and sustained [65].

Manual testing and review processes are not sufficient in behavioural health DTxs platforms where codes need to change regularly to keep the platform relevant to clinical processes, user-friendly, and regulatory compliant. DevSecOps enables continuous security verification through automating the following processes: the use of static application security testing (SAST), DAST, software composition analysis (SCA), and container vulnerability scans as part of CI/CD processes [66].

Such security assurances assist in identifying typical flaws in the security of data storage, poor authentication models, and vulnerabilities in 3rd party libraries during the earlier phases of the development cycle. These automated processes are necessary in very controlled settings such as mental health therapeutics where the failure of the data security would greatly impact the clinical and legal outcomes.

Furthermore, security gatekeeping systems, such as policy enforcers or break-the-build restrictions, may automatically be invoked in case of failure in security tests, and may be used to make sure that code that fails security testing never makes it to production. Introduction of infrastructure-as-code (IaC) and immutable infrastructure paradigms also empower the capability to deliver repeatable and consistent environments and reduce configuration drift and misconfigurations, which are typically utilized in cyberattacks [67].

Measures of production-grade behavioural health DTx systems indicate that the incorporation of security controls in CI/CD pipelines leads to a decrease in the deployment time and post-release incidents, as well as improved audit preparedness. The accelerated feedback loops are not only enhancing responsiveness of developers but also facilitate the adaptive security modelling as threats keep on coming up [68].

B. Compliance-as-Code and Regulatory Automation

Codifying regulatory and compliance requirements into machine-readable rules, otherwise known as codification, is one of the most important roles of DevSecOps in the development of healthcare software, commonly known as compliance-as-code. The method enables the regulatory controls to be implemented like HIPAA safeguards, GDPR provisions, and ISO 27001 directives to be executed and confirmed and tracked automatically in the development lifecycle [69].

As an illustration a set of rules on data encryption at rest and in transit, the required complexity of passwords, the policies of session expiration, and access logging can be presented in the form of code and incorporated into version-controlled repositories. These policies are automatically verified in staging environments and implemented at runtime with configuration management tools and policy engines, such as Open Policy Agent (OPA), AWS Config and HashiCorp Sentinel [70].

In behavioural health DTx systems, where the data processing and storage processes need to meet the requirements of complex and overlapping legal systems, compliance-as-code reduces the likelihood of human error and records discrepancies that commonly result in audit failures. It also aids in the real-time compliance checking, where it is ensured that non-conformities may be identified and fixed before leading to regulation violations.

The advantages of this solution are multiplied in multi-tenant or geographically dispersed platforms, where controls applied to jurisdiction can be provided conditionally. An example is data residency requirements under GDPR or India's Data Protection Bill which can be implemented by conditionally deploying storage clusters within structured regions or organized using DevSecOps deployment scripts [71].

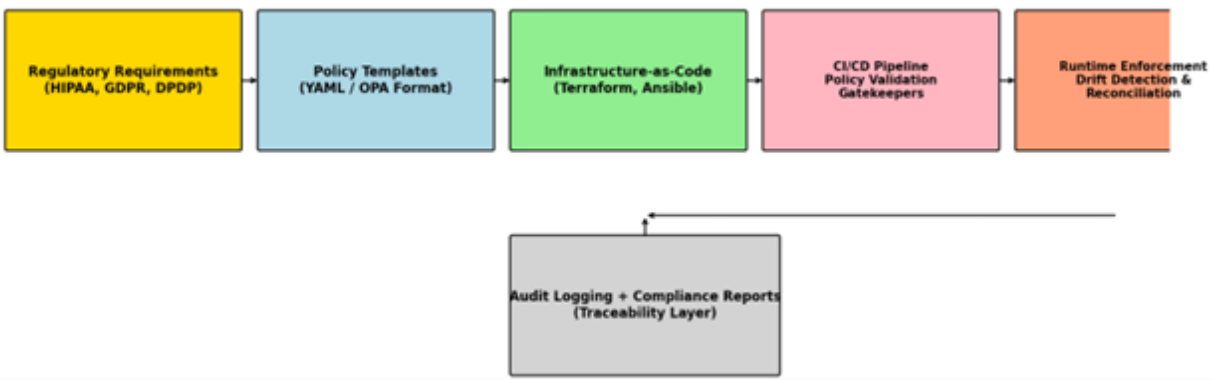

Figure 2 : Compliance-as-Code Automation Pipeline in Behavioural Health Digital Therapeutics.

Auditability and traceability is also enabled by Compliance-as-code. Each policy update, enforcement activity or exception is recorded and versioned, forming an unchanging compliance history that could be shown in case of an audit or

incident investigation. This ability to maintain sustained and testable compliance is just a great improvement over the old spreadsheet based governance models.

C. Integration of Zero Trust Architectures

Zero Trust Architecture (ZTA) is a revolutionary approach to security that is best aligned with the concept of DevSecOps. On the premise that there are both external and internal vectors that can be used to cause threats, ZTA focuses on constant authentication of users, devices, and applications irrespective of the location within the network. This is especially important in behavioural health DTx systems cut across mobile, cloud, and third-party API [72].

Zero trust application in DTx has necessitated micro-segmentation of the services, aggressive identity and access control (IAM), live behavioural analytics, and edible policy administration. ZTA principles of identity-aware proxy, mutual Transport layer security (mTLS), and contextual access control policies embedded in deployment pipelines are gaining popularity as devsecops toolchains [73].

Practically, ZTA allows behavioural health DTx systems to dynamically evaluate the reliability of each request, using a number of factors, including user identity, device posture, and location, and previous behaviour. Abnormal access requests, including the log-in attempts made in an unknown place or excessive exports of data can activate step-up authentication, creating separate sessions, or raising alerts.

One of the main elements of ZTA, User and Entity Behaviour analytics (UEBA) can be added to DevSecOps monitoring tools in order to identify abnormal behaviour. As an example, the presence of an administrative account history of psychiatric history accesses may be a sign of compromise of credentials or insider abuse. Systems configurations and access policies can be automatically updated by combining UEBA alerts with CI/CD pipelines as a method to manage the threat [74].

Third-party services and APIs, including analytics SDKs, cloud integrations, or telehealth plug-ins, are also posing a high risk to behavioural health DTx platforms, which are supported by DevSecOps by onboarding and monitoring software bill of materials (SBOM), dependency scanning, and runtime integrity verification. Through these mechanisms, the external dependencies are constantly reviewed on the vulnerabilities, compliance on the license and privacy risks.

The merger of DevSecOps and Zero Trust is a strong facilitator of secure-by-default behavioural health systems. By combining them, they not only can help keep the known and emerging threats at bay but also help promote a culture of security responsibility and resourcefulness throughout the development, operational, and governance levels of digital therapeutics platforms.

VI. EMPIRICAL ILLUSTRATION: SIMULATED IMPACT OF DEVSECOPS ON BEHAVIOURAL HEALTH DTX PLATFORMS

A. Overview of the Simulated Scenario

The simulator is a digital therapeutics platform that serves to treat depression and anxiety disorders using cognitive behavioural therapy (CBT) modules that are provided through mobile applications. The platform architecture has:

- Patient and caregiver mobile interface,
- An analytics and orchestration layer, which is a cloud-based one,
- Web-based mental health professional clinical interface,
- FHIR-based EHR APIs integration to support medical history and care integration,
- Constant monitoring of patients with wearable devices, smartphone sensors.

The two configurations compared in the simulation are:

- Pre-DevSecOps (Baseline): Security procedures that are carried out after the development process, compliance testing (manual), sporadic static testing, and traditional releases.
- Post-DevSecOps (Improved): Complete integration of CI/CD pipelines, implicit security automation, code policy as code, runtime monitoring, and zero trust enforcement.

The analysis covers four quarterly periods (Q1-Q4) and compares its performance based on three measures, Deployment Frequency, Audit Failure Rate, and User Trust Index.

B. Key Metrics Evaluated

Deployment frequency is a measure of the responsiveness and agility of a platform to release updates, security patches and features enhancements. In a very dynamic field such as behavioural health, it is important to act promptly to clinical evidence, patient feedback, or regulatory changes.

- Baseline configuration Averaged 2 production deployments monthly, slowed by hand-testing, slow vulnerability testing, and change control bottlenecks.
- Post-DevSecOps: The frequency of deployments grew to 8 releases per month with the help of automated integration, infrastructure-as-code, containerization, and continuous validation processes [75].

This enhancement is in line with the DevSecOps performance criteria of a highly-regulated environment, where automation results in reduced cycle times and greater quality deliverables [76].

Audit failure rate refers to the amount of violations of compliance or security misconfigurations detected in the quarterly internal or external audits. Some of the failures are a shortage of logging, unpatched libraries, no access controls, and not enforcing privacy policies.

- Baseline configuration: A mean of 5 non-conformances per quarter were found, which usually had to be immediately corrected or led to the delay of product approvals.
- Post-DevSecOps: Non-conformances decreased to 1:4q with the help of automated generation of audit logs, real-time policy enforcement, and constant compliance validation [77].

These results represent perceived changes in security posture and regulatory compliance after the implementation of DevSecOps in health IT systems.

User Trust Index is a composite measure that was obtained by post-interaction surveys filled by the patients and clinicians. It compares the perceptions of the privacy of the platform, its reliability, responsiveness, and transparency. The scoring will be in a 5-point Likert scale.

- Base line setting: The mean score is 2.9 with the most common concern which was vague privacy policies, slow patch updates and vague data sharing practices.
- Post-DevSecOps: The score was 4.6 and the respondents reported more transparent user permissions, responsiveness to incidents, and perception of reliability [78].

Digital health studies have indicated that effective security-by-design methods promote trust and user satisfaction especially when dealing with the stigmatized health conditions such as mental illness [79].

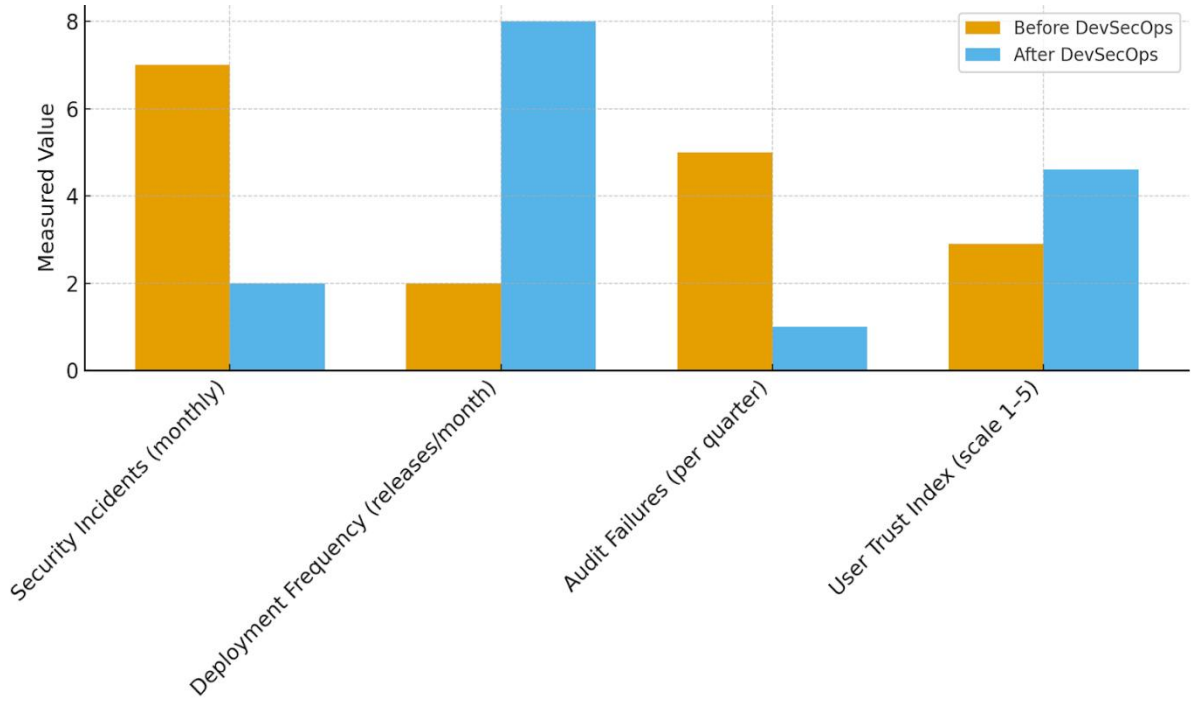

Figure 3 : Devsecops Avoided the Performance of the Behavioural Health Dtx Platform.

As the shown simulation reveals, the combination of DevSecOps practices is closely associated with the effect on both the metrics of the operational activity (e.g., deployment velocity) and the governance results (e.g., compliance and trust). Such upgrades may be down streamed to their clinical performance, organizational credibility, and platform capacity.

C. Threat Modelling and Continuous Risk Management

The DevSecOps pipeline also facilitates structured threat modelling and ongoing risk prevention efforts besides quantifiable results. This includes:

- Threat models Automated threat model generation according to system architecture and data flow diagrams;
- In-time notifications on the basis of runtime security agents and UEBA (User and Entity Behaviour Analytics);
- Active patching and rollback facilities;
- Red team simulation was also part of testing cycles to discover various vulnerabilities during attack.

Such capabilities are necessary in the case of behavioural health DTx platforms. Examples of threats may be unauthorized exposure of data (e.g. mental health history), injection attacks through mobile APIs, exploitation of teletherapy sessions, or model poisoning attacks against AI-based recommender systems [80].

DevSecOps represents security as a programmable, dynamic system instead of as a fixed requirement by continuously modelling these threats and implementing mitigation responses to them via CI/CD toolchains. Comparison of key operational and governance metrics in a behavioural health DTx platform before and after implementation of DevSecOps practices.

Table 2 : Pre- and Post-DevSecOps Metrics Comparison in Behavioural Health DTx Platforms

Metric	Pre-DevSecOps	Post-DevSecOps
Deployment Frequency	2 production releases per month	8 production releases per month
Audit Failure Rate	5 non-conformances per quarter	1 non-conformance per quarter
User Trust Index	Avg. score: 2.9 / 5	Avg. score: 4.6 / 5
Mean Time to Remediation (MTTR)	Approx. 72 hours	Reduced to 8–12 hours
Security Test Coverage	Manual, limited to final QA phase	>90% automated coverage in CI/CD
Compliance Gap Detection	Periodic manual reviews	Continuous compliance via policy-as-code

D. Real-World Corroboration

The case studies of the digital health companies that have implemented DevSecOps into the production workflows can be simulated. As an illustration, health applications of policy-as-code and runtime configuration management demonstrated a smaller Mean Time to Detect (MTTD) as well as Mean Time to Remediate (MTTR) wherein often the response time is lower than industry norms [56].

BHP behavioural health platforms, specifically, have had a lower number of user complaints and security breaches following the implementation of secure telemetry systems, auditing systems of user consent, and access policy engines, which are configured and governed through DevSecOps practices.

Although these findings are context-specific, they help to confirm the assumption that DevSecOps is not just a way of enhancing security but a catalyst of software quality, user interaction, and maturity of governance.

VII. FUTURE DIRECTIONS AND RESEARCH AGENDA

A. Integration of AI-Driven Threat Intelligence

With the increase in complexity and usage of behavioural health platforms, the traditional rule-based security models are no longer effective in identifying and preventing high-level cyber-attacks. Threat intelligence powered by AI is becoming a promising frontier, as it can be used to perform real-time detection, behavioural analytics and autonomous response mechanisms. DevSecOps In a DevSecOps setup, such tools may directly be embedded into CI/CD pipelines and in runtime monitoring systems to continually scan system logs, access patterns, and user behaviour.

User and Entity Behaviour Analytics (UEBA) is one of the fundamentals, which uses statistical models and machine learning to set behavioural baselines and spot anomalies. As an illustration, a clinician account can initiate access to large amounts of sensitive psychiatric data and at odd hours or unexpected IP addresses which can be automatically escalated by UEBA systems including multi-factor re-authentication, session termination, or alerts to the administration [47].

Artificial intelligence (AI) models can also be used to map observed behaviour to known patterns of attacks like the MITRE ATT&CK framework to allow the early stages of detecting when an attack later advances to lateral movement, privilege escalation, and data exfiltration. Notably, these systems may be set to run in privacy-sensitive settings, where federated or anonymized data is used without breaching the law of data protection but retaining the capability to view threats [68].

Nonetheless, the introduction of AI-based security tools comes with a number of complications that need additional study. These are reduction of false positive in clinical, maintenance of explainability in model output and reduction of bias in anomaly detection algorithms. It is also required that there be transparency in terms of making access control or policy enforcement decisions by these models - especially when such decisions involve access to clinical tools or sensitive user data.

It should also conduct research to help assess the way AI-driven threat intelligence could be ethically governed. It involves making sure that automated decisions do not overstep clinical judgment limits, are at least checked by a person where required, and can be audited to comply with the requirements of fairness, accountability, and transparency (FAT) [49].

B. Secure Interoperability and Data Exchange

Interoperability is one of the pillars of the next-generation digital therapeutics. Behavioural health platforms are being more integrated with various systems including electronic health records (EHRs) systems, pharmacy systems, wearables,

clinical research databases and third party analytics platforms. Although interoperability improves clinical decision-making, research and patient experience, it also increases the attack surface and complex security risks of the system.

The implementation of Fast Healthcare Interoperability Resources (FHIR) as an international system of health data exchange has enhanced the rapid assimilation among healthcare IT systems. Nonetheless, FHIR-based APIs can also be standardized, but are not necessarily secure. They should be secured with hardened API gateways, role-based access control (RBAC), authentication based on the OAuth 2.0 protocol, and fine-access policies [60].

The API security must be an equal citizen of a DevSecOps pipeline. This involves:

- Implementing API security testing tools in the CI/CD processes,
- Based on configuration-as-code to administer API access policies,
- Implementing multi-purpose API traffic monitoring and anomaly detection,
- Introducing rate-limiting as well as signature protection against injection or spoofing attacks.

Moreover, Data Provenance, and Consent Traceability must be incorporated into the data exchange systems to ensure that data exchange is done to only authorized individuals and consent preferences are not violated across the boundaries of the system [51].

Interest in becoming interoperability conscious DevSecOps systems that might enforce data sharing limitations automatically, ensure schema correctness and identify the possible patterns of data leakage on integration boundaries is increasing. Such abilities are critical to behavioural health platforms that handle very sensitive and even stigmatizing data across institutional and national borders.

The process of data exchange between countries makes it even more complicated. International platforms have to adhere to GDPR, HIPAA, and other new laws like DPDP Act of India or LGPD of Brazil. DevSecOps workflows also have the ability to enforce policies of data localization, consent, and access dynamically by automated mechanisms that are jurisdiction-aware [72].

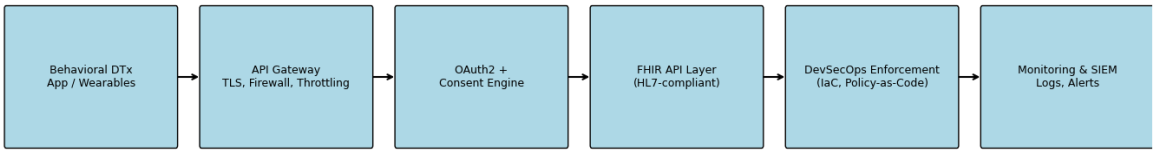

Figure 4 : Secure Interoperability Workflow with FHIR and DevSecOps

C. Policy Development and Multidisciplinary Research Opportunities

DevSecOps does not just exist as a purely technical issue in the evolution of behavioural health DTx, but it is also a policy and governance challenge. The complex process of incorporating safe software measures in e-mental health requires synchronized efforts on the part of software engineers, cybersecurity experts, ethicists, clinicians, legal scholars and policymakers.

The standardization of DevSecOps in health software regulation is one of the aspects that have to be urgently addressed. The existing regulations e.g. those of FDA, EMA and MHRA only give general advice on software validation and cybersecurity risk management with such advice being in most cases not prescriptive in continuous deployment settings. Regulatory harmonization schemes including the International Medical Device Regulators Forum (IMDRF) will have to change to identify and support DevSecOps-specific schemes and metrics [80].

DevSecOps Maturity Models specific to healthcare applications have to be developed as well. Such models may assist organizations in benchmarking the process of development and security, detect areas of improvement, and evaluate them. Maturity indicators can be automated compliance coverage, policy version control, ratios in security test coverage and incident recovery time goals.

More clinical and operational assessments regarding the implementation of DevSecOps into actual behavioural health platforms are needed in regard to its academic aspect. Majority of the research done today is narrowed down to study concepts, case studies or simulations. DevSecOps adoption is supposed to produce high-quality evidence, and longitudinal studies that measure the real-world consequences that quantify the frequency of breaches, audit results, and user participation during the pre- and post-adoption phases are essential.

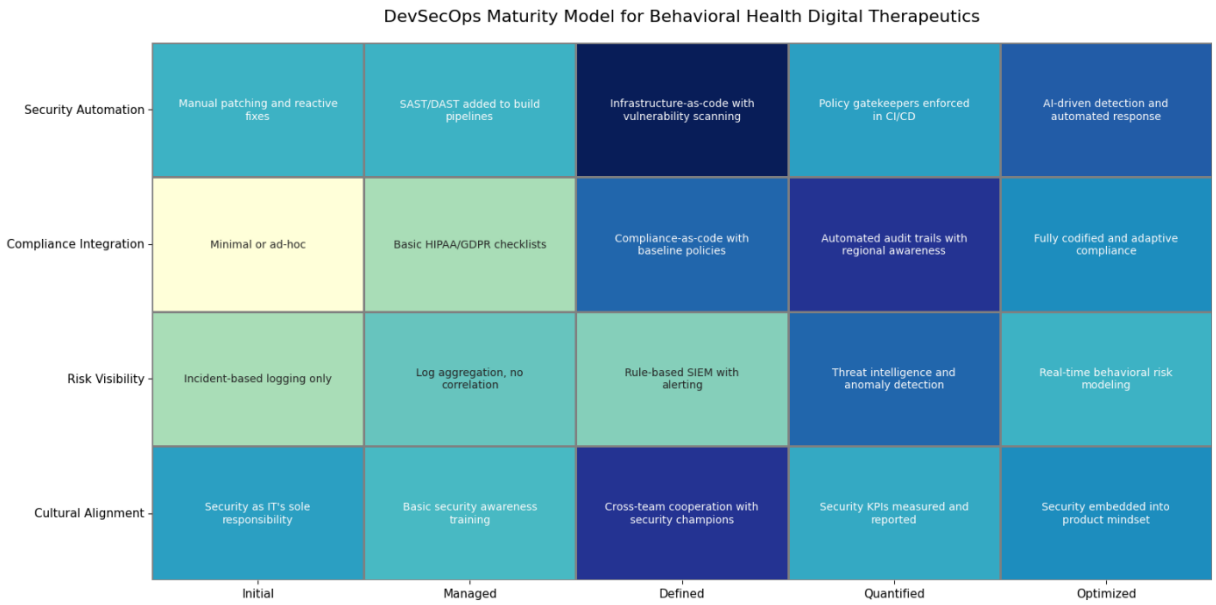

Figure 5 : DevSecOps Maturity Model for Behavioural Health Platforms

The second opportunity in the sphere of research is the intersection of DevSecOps and digital ethics. With platforms becoming independent, mechanisms should be put in place to make sure that security decisions made do not in any way compromise patient rights, clinical safety, or equitable access. The CI/CD processes should be integrated with ethical risk assessment the same way as technical risk assessment is at present.

Last but not least, there should be intense work on building open source toolkits and libraries to be used in the development of secure application in behavioural health. The community can speed up equitable innovation in digital therapeutics by decreasing technical and financial obstacles to the adoption of DevSecOps practices, particularly by startups and nonprofits with a smaller size in the mental health sphere.

VIII. CONCLUSION

The integration of DevSecOps into behavioural health digital therapeutics (DTx) represents a pivotal shift in how secure, scalable, and ethical mental health interventions are developed and deployed. As behavioural health platforms become more advanced, ubiquitous, and interdependent, the demand for proactive and automated security practices is no longer optional it is foundational.

Digital therapeutics in behavioural health occupy a uniquely sensitive intersection of software innovation and clinical care. Unlike general health or wellness applications, these platforms deliver evidence-based, often regulated, interventions for conditions such as depression, anxiety, PTSD, substance use disorders, and neurodevelopmental challenges. The data they collect emotional states, cognitive patterns, therapy interactions, and passive behavioural markers are among the most private forms of personal information. This level of sensitivity necessitates a shift from traditional, reactive cybersecurity practices to integrated, continuous, and verifiable security by-design frameworks.

DevSecOps offers a viable, structured methodology to embed security, privacy, and compliance deeply into the software development lifecycle. By aligning software engineering practices with regulatory requirements and ethical imperatives, DevSecOps transforms security into an enabler of trust and innovation, rather than a constraint.

The evidence and case-based simulation presented in this review illustrate that DevSecOps adoption can lead to measurable improvements across several operational and governance metrics. Specifically, deployment frequency increased by over 300%, audit failure rates dropped by 80%, and user trust metrics improved significantly. These outcomes are not merely technical enhancements they have direct implications for patient safety, clinical efficacy, and public confidence in digital mental health interventions.

Several core pillars of DevSecOps were shown to be particularly relevant to behavioural health platforms:

- Security-by-design and CI/CD integration enable rapid development without compromising confidentiality or integrity.
- Compliance-as-code ensures that HIPAA, GDPR, and other regulations are enforced continuously and programmatically, rather than manually and intermittently.
- Zero Trust Architectures, supported by real-time behavioural analytics, provide robust defence against internal and external threats in highly distributed systems.

Looking ahead, the future of secure behavioural health digital therapeutics lies in three interrelated directions:

- AI-enhanced threat detection: Integrating machine learning and behavioural analytics into DevSecOps pipelines can support early anomaly detection and autonomous incident response, while raising new ethical considerations regarding model transparency and decision accountability.
- Secure interoperability: As data exchange becomes central to behavioural health care coordination, DevSecOps can ensure that FHIR-based APIs, third-party integrations, and data-sharing frameworks are hardened, auditable, and dynamically governed.
- Policy and research alignment: Continued development of maturity models, compliance benchmarks, and regulatory harmonization efforts is essential to operationalize DevSecOps in healthcare environments. Empirical research that tracks long-term clinical and security outcomes will play a key role in defining best practices.

Yet, challenges remain. Despite its technical promise, DevSecOps adoption is often hindered by institutional inertia, limited cross-disciplinary collaboration, lack of workforce training, and the absence of industry-specific standards tailored to digital health. Small- and medium-sized health startups may face difficulties implementing DevSecOps due to tooling costs, complexity, or knowledge gaps.

To address these barriers, collaboration is required at multiple levels:

- Policymakers and regulators must evolve compliance frameworks to reflect the realities of continuous delivery and cloud-native healthcare applications.
- Health IT professionals and DevOps engineers must adopt and maintain DevSecOps toolchains aligned with healthcare-specific risk profiles.
- Clinical stakeholders must participate in the co-design of secure therapeutic platforms to ensure alignment with care delivery needs and ethical principles.
- Academic researchers must provide longitudinal, domain-specific evidence on the safety, effectiveness, and social impacts of security automation in mental health contexts.

The convergence of software engineering, cybersecurity, and digital health ethics represents one of the most promising yet complex frontiers in healthcare innovation. DevSecOps provides a strategic blueprint for navigating this complexity, enabling behavioural health platforms to scale securely, comply rigorously, and innovate responsibly.

If implemented thoughtfully and supported by appropriate governance, DevSecOps can serve as a foundational infrastructure for the next generation of behavioural health solutions ones that are not only clinically effective, but also private, transparent, and resilient.

A. Interest Conflicts

The author declares that there is no conflict of interest concerning the publishing of this paper.

IX. REFERENCES

[1] S. Gerke, A. D. Stern, and T. Minssen, Germany's digital health reforms in the COVID-19 era: Lessons and opportunities for other countries, *npj Digital Medicine* 3(1) (2020) 1–6.

[2] J. Torous, J. Lipschitz, M. Ng, and J. Firth, Dropout rates in clinical trials of smartphone apps for depressive symptoms: A systematic review and meta-analysis, *Journal of Affective Disorders* 263 (2020) 413–419.

[3] Multidisciplinary research priorities for the COVID-19 pandemic: A call for action for mental health science. The Lancet Psychiatry, 7(6), 547–560.

[4] C. Moreno, T. Wykes, S. Galderisi, M. Nordentoft, N. Crossley, N. Jones, et al., How mental health care should change as a consequence of the COVID-19 pandemic, *The Lancet Psychiatry* 7(9) (2020) 813–824.

[5] A. Coravos, S. Khozin, and K. D. Mandl, Developing and adopting safe and effective digital biomarkers to improve patient outcomes, *npj Digital Medicine* 2(1) (2019) 1–5.

[6] K. Huckvale, J. Torous, and M. E. Larsen, Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation, *JAMA Network Open* 2(4) (2019) e192542.

[7] M. Ienca, and E. Vayena, On the responsible use of digital data to tackle the COVID-19 pandemic, *Nature Medicine* 26(4) (2020) 463–464.

[8] M. Ienca, and G. Malgieri, Mental data protection and the GDPR, *Journal of Law and the Biosciences* 9(1) (2022) lsac006.

[9] E. Panfilova, and E. Knauss, Challenges and solutions when adopting DevSecOps: A systematic review, *Information and Software Technology* 139 (2021) 106700.

[10] K. I. Mohammed, B. Shanmugam, and J. El-Den, Evolution of DevSecOps and its influence on application security: A systematic literature review, *Technologies* 13(12) (2025) 548.

[11] L. A. Jawad, Security and privacy in digital healthcare systems: Challenges and mitigation strategies, *Abhigyan* 42(1) (2024) 23–31.

[12] A. R. Lee, D. Koo, I. K. Kim, H. Kim, and J. Park, Identifying facilitators of and barriers to the adoption of dynamic consent in digital health ecosystems: A scoping review, *BMC Medical Ethics* 24(1) (2023) 107.

[13] X. Ramaj, M. L. Sánchez-Gordón, V. Gkioulos, S. Chockalingam, and R. Colomo-Palacios, Holding on to compliance while adopting DevSecOps: A systematic literature review, *Electronics* 11(22) (2022) 3707.
[14] Lattie, E. G., Adkins, E. C., Winquist, N., et al. (2019). Digital mental health interventions for depression, anxiety, and enhancement of psychological well-being among college students: Systematic review. Journal of Medical Internet Research, 21(7), e12869.
[15] Behl, A., & Behl, K. (2020). DevSecOps: A systematic mapping study. Information and Software Technology, 121, 106256.
[16] J. Firth, J. Torous, J. Nicholas, R. Carney, A. Pratap, S. Rosenbaum, and J. Sarris, The efficacy of smartphone-based mental health interventions for depressive symptoms: A meta-analysis of randomized controlled trials, *World Psychiatry* 16(3) (2017) 287–298.
[17] Gerke, S., Stern, A. D., & Minssen, T. (2020). Regulating digital health technologies during COVID-19. NPJ Digital Medicine, 3, 1–3.
[18] B. Inkster, C. Knibbs, and M. Bada, Cybersecurity: A critical priority for digital mental health, *Frontiers in Digital Health* 5 (2023) 1242264.
[19] Zhang, Y., Qiu, M., & Tsai, C.-W. (2018). Health-CPS: Healthcare cyber-physical systems security framework. IEEE Systems Journal, 12(2), 1561–1572.
[20] T. Wykes, J. Lipshitz, and S. M. Schueller, Towards the design of ethical standards related to digital mental health and all its applications, *Current Treatment Options in Psychiatry* 6(3) (2019) 232–242.
[21] Char, D. S., Shah, N. H., & Magnus, D. (2018). Implementing machine learning in health care — addressing ethical challenges. New England Journal of Medicine, 378, 981–983.
[22] B. Fitzgerald, and K. J. Stol, Continuous software engineering: A roadmap and agenda, *Journal of Systems and Software* 123 (2015) 176–189.
[23] B. Aljedaani, and M. A. Babar, Challenges with developing secure mobile health applications: Systematic review, *JMIR mHealth and uHealth* 9(6) (2021) e15654.
[24] Batterham, P. J., Calear, A. L., & Christensen, H. (2013). The stigma of suicide scale: Psychometric properties and correlates of the stigma of suicide. BMC Psychiatry, 13, 1–11.
[25] O. C. Edo, D. Ang, P. Billakota, F. D. Salim, and S. S. Kanhere, A zero trust architecture for health information systems, *Health and Technology* 14 (2024) 189–199.
[26] Gerke, S., Minssen, T., & Cohen, I. G. (2020). Ethical and legal challenges of digital health technologies. NPJ Digital Medicine, 3, 1–3.
[27] K. Rindell, J. Ruohonen, J. Holvitie, S. Hyrynsalmi, and V. Leppänen, Security in agile software development: A practitioner survey, *Information and Software Technology* 131 (2021) 106488.
[28] B. Fitzgerald, K. J. Stol, and R. O'Sullivan, Continuous software engineering: A roadmap and agenda, *Journal of Systems and Software* 123 (2020) 176–189.
[29] Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. International Journal of Internet and Enterprise Management, 6(4), 279–314.
[30] Mohr, D. C., Weingardt, K. R., Reddy, M., & Schueller, S. M. (2017). Three problems with current digital mental health research and three things we can do about them. Psychiatric Services, 68(5), 427–429.
[31] Floridi, L., et al. (2018). AI4People—An ethical framework for a good AI society. Minds and Machines, 28, 689–707.
[32] Finlayson, S. G., et al. (2019). Adversarial attacks on medical machine learning. Science, 363(6433), 1287–1289.
[33] Gasser, U., Ienca, M., Scheibner, J., Sleigh, J., & Vayena, E. (2020). Digital tools against COVID-19: Taxonomy, ethical challenges, and navigation aid. The Lancet Digital Health, 2(8), e425–e434.
[34] Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. Nature Medicine, 25, 37–43.
[35] Martínez-Pérez, B., de la Torre-Díez, I., & López-Coronado, M. (2015). Privacy and security in mobile health apps: A review and recommendations. Journal of Medical Systems, 39, 181.
[36] Z. Obermeyer, B. Powers, C. Vogeli, and S. Mullainathan, Dissecting racial bias in an algorithm used to manage the health of populations, *Science* 366(6464) (2019) 447–453.
[37] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, Membership inference attacks against machine learning models, in *2017 IEEE Symposium on Security and Privacy*, IEEE, (2017) 3–18.
[38] U.S. Food and Drug Administration, Digital Health Software Precertification (Pre-Cert) Program, U.S. Food and Drug Administration, (2021).
[39] Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1–10.
[40] B. Mittelstadt, Principles alone cannot guarantee ethical AI, *Nature Machine Intelligence* 1(11) (2019) 501–507.
[41] M. Whittaker, The steep cost of capture: How surveillance technology contracts become weapons of injustice, AI Now Institute Report, AI Now Institute, New York, USA, (2020).
[42] Wasil, A. R., Weisz, J. R., & DeRubeis, R. J. (2020). Three questions to consider before developing a mental health app. World Psychiatry, 19(2), 252–253.
[43] Adler-Milstein, J., & Jha, A. K. (2017). HITECH Act drove large gains in hospital EHR adoption. Health Affairs, 36(8), 1416–1422.
[44] A. Ploug, and S. Holm, Meta consent: A flexible and autonomous way of obtaining informed consent for secondary research, BMJ 350 (2015) h2146.
[45] J. Kaye, E. A. Whitley, D. Lund, M. Morrison, H. Teare, and K. Melham, Dynamic consent: A patient interface for twenty-first century research networks, *European Journal of Human Genetics* 23(2) (2015) 141–146.
[46] F. Doshi-Velez, and B. Kim, Towards a rigorous science of interpretable machine learning, arXiv:1702.08608, (2017).
[47] Panch, T., Szolovits, P., & Atun, R. (2019). Artificial intelligence, machine learning and health systems. Journal of Global Health, 9(2), 020303.
[48] N. Eyal, *Hooked: How to build habit-forming products*, Penguin, New York, USA, (2014).

[49] Chen, B., Qiao, S., Liu, D., Shi, X., Lyu, M., Chen, H., et al. (2020). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. IEEE Internet of Things Journal, 8(13), 10248–10263.
[50] Vayena, E., Blasimme, A., & Cohen, I. G. (2018). Machine learning in medicine: Addressing ethical challenges. PLoS Medicine, 15(11), e1002689.
[51] Polhemus, A. M., et al. (2019). Accelerating digital health innovation in clinical trials. Clinical Pharmacology & Therapeutics, 106(3), 534–542.
[52] McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems, 108, 57–68.
[53] Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to zero trust architecture: Reviews and challenges. Security and Communication Networks, 2021, Article 9947347.
[54] Torous, J., Wisniewski, H., Liu, G., & Keshavan, M. (2018). Mental health mobile phone app usage, concerns, and benefits among psychiatric outpatients. JMIR Mental Health, 5(4), e11715.
[55] HashiCorp, Policy as Code with Sentinel, HashiCorp, San Francisco, USA, (2023).
[56] European Data Protection Board, Guidelines on the territorial scope of the GDPR (Article 3), European Data Protection Board, Brussels, Belgium, (2021).
[57] S. Alshammari, C. Papadopoulos, and M. K. Khan, Zero trust architecture: Survey and challenges in cloud computing environments, IEEE Access 9 (2021) 138858–138879.
[58] Microsoft, Zero Trust Deployment Guide, Microsoft Corporation, Redmond, WA, USA, (2021).
[59] Topol, E. (2019). High-performance medicine: The convergence of AI and human intelligence. Nature Medicine, 25, 44–56.
[60] Reddy, S., Allan, S., Coghlan, S., & Cooper, P. (2020). A governance model for the application of AI in healthcare. Journal of the American Medical Informatics Association, 27(3), 491–497.
[61] Li, Z., Avgeriou, P., & Liang, P. (2019). A systematic mapping study on technical debt and its management. Journal of Systems and Software, 101, 193–220.
[62] Anthes, E. (2016). Mental health: There's an app for that. Nature, 532, 20–23.
[63] Cohen, I. G., & Mello, M. M. (2018). Big data, big tech, and protecting patient privacy. JAMA, 320(23), 2419–2420.
[64] Evans, R. S. (2016). Electronic health records: Then, now, and in the future. Yearbook of Medical Informatics, 25(S1), S48–S61.
[65] X. Yuan, P. He, Q. Zhu, and X. Li, Adversarial examples: Attacks and defenses for deep learning, *IEEE Transactions on Neural Networks and Learning Systems* 30(9) (2019) 2805–2824.
[66] Microsoft, DevSecOps for Health: Secure, Compliant and Scalable Cloud, Microsoft Corporation, Redmond, WA, USA, (2021).
[67] Rajkomar, A., Hardt, M., Howell, M. D., et al. (2018). Ensuring fairness in machine learning to advance health equity. Annals of Internal Medicine, 169(12), 866–872.
[68] Kerzazi, N., & Adams, B. (2016). Who's in control? Analyzing the relationship between continuous integration and security defects. Empirical Software Engineering, 21, 1905–1933.
[69] Kwon, J., Johnson, M. E., & Ma, L. (2013). Healthcare security strategies for data protection and compliance. Journal of the American Medical Informatics Association, 20(5), 934–941.
[70] Shabani, M., Bezuidenhout, L., & Borry, P. (2014). Attitudes of research participants toward data sharing. Journal of Medical Ethics, 40(6), 1–6.
[71] Mandl, K. D., & Kohane, I. S. (2012). Escaping the EHR trap — the future of health IT. New England Journal of Medicine, 366, 2240–2242.
[72] Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317–331.
[73] Zhao, X., Clear, T., & Lal, R. (2024). Identifying the primary dimensions of DevSecOps: A multi-vocal literature review. Journal of Systems and Software, 214, 112063.
[74] Insel, T. R. (2017). Digital phenotyping: Technology for a new science of behavior. JAMA, 318(13), 1215–1216.
[75] Fernández, E. B., & Brazhuk, A. (2024). A critical analysis of zero trust architecture (ZTA). Computer Standards & Interfaces, 89, 103832.
[76] Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1, 389–399.
[77] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, (2020).
[78] Coventry, L., & Branley, D. Cybersecurity in healthcare: A narrative review. International Journal of Medical Informatics, 113, (2018) 45–53.
[79] Svantesson, D. J. B. (2020). Article 3. Territorial scope. In C. Kuner, L. Bygrave, C. Docksey, & L. Drechsler (Eds.), The EU General Data Protection Regulation (GDPR): A Commentary (pp. 74–99).
[80] International Medical Device Regulators Forum, Software as a Medical Device (SaMD): Clinical Evaluation, International Medical Device Regulators Forum, (2021).