Requirements-Driven Evaluation of Model-Based Low-Code Platforms for GDPR-Compliant Health Applications: A Comparative Study of Mendix and OutSystems

Sofia Meacham[1][a], Chukwuebuka Obiora[1]
[1] *School of Computing & Engineering,Bournemouth University , Fern Barrow, Poole, UK*
smeacham@bournemouth.ac.uk, s5712784@bournemouth.ac.uk

Keywords: Low-Code Platforms, GDPR, Mendix, OutSystems, Requirements Engineering, Digital Health, Compliance Evaluation

Abstract: Low-code/no-code (LCNC) platforms are increasingly promoted for healthcare applications, enabling non-technical professionals to prototype digital solutions. In regulated domains, however, compliance with the General Data Protection Regulation (GDPR) is critical, and it is unclear whether LCNC platforms provide adequate support for such requirements. This paper introduces a requirements-driven evaluation framework that operationalises five GDPR provisions—data minimisation (Art. 5), lawfulness of processing (Art. 6), consent (Art. 7), privacy by design/default (Art. 25), and security of processing (Art. 32)—into concrete modelling tasks. The framework is applied in a comparative study of two leading LCNC platforms, Mendix and OutSystems, using a benchmark chronic disease management application. Findings show that Mendix offers more accessible support for non-technical users, particularly for consent and privacy-by-default, while OutSystems provides greater flexibility in data handling at the cost of higher configuration effort. The study contributes a structured framework for linking legal obligations to model-based development tasks and provides practical insights for selecting LCNC platforms in GDPR-regulated healthcare contexts.

1 INTRODUCTION

Model-based software and systems engineering techniques are increasingly adopted in healthcare to accelerate the development of digital solutions such as mobile health applications, decision-support dashboards, and remote monitoring tools. These innovations promise improvements in interoperability, patient engagement, and personalised care. Yet their deployment is often hindered by slow development cycles, overburdened IT teams, and strict data protection obligations. The General Data Protection Regulation (GDPR) (European Union, 2016) adds further complexity by requiring developers to implement data minimisation, lawful processing, consent capture and withdrawal, privacy by design, and secure processing of sensitive health data.

Low-code/no-code (LCNC) platforms provide a potential solution by allowing non-technical "citizen developers," including medical professionals, to create applications using visual modelling environments and drag-and-drop logic. Industry studies suggest LCNC approaches can reduce development time by up to 90% compared to traditional coding (Gartner, 2021). However, while vendors advertise compliance-ready features, little evidence exists on how accessible and effective these mechanisms are for non-technical users.

This paper addresses that gap by presenting a requirements-driven evaluation of two widely adopted LCNC platforms—Mendix (Mendix, 2025) and OutSystems (OutSystems, 2025)—against key GDPR provisions. A benchmark chronic disease management application was implemented on both platforms to test whether GDPR requirements can be realised without extensive developer input. The contributions of this paper are:

1. **A requirements-driven evaluation framework** that translates five GDPR provisions—data minimisation (Art. 5), lawfulness of processing (Art. 6), consent (Art. 7), privacy by design and default (Art. 25), and security of processing (Art. 32)—into concrete modelling tasks suitable for low-code/no-code (LCNC) environments.
2. **An empirical illustration of the framework**

[a] https://orcid.org/0000-0002-8474-4917

through a comparative study of two widely adopted LCNC platforms, Mendix and OutSystems, using a benchmark chronic disease management application.

3. **Practical insights for healthcare innovation**, showing how Mendix and OutSystems differ in accessibility for non-technical professionals: Mendix supports more intuitive consent and privacy features, while OutSystems provides greater flexibility at higher configuration cost.

Together, these contributions demonstrate how regulatory requirements can be systematically operationalised into model-based development tasks and used to assess the compliance readiness of LCNC platforms in regulated domains.

The remainder of this paper is organised as follows. Section 2 reviews background work on low-code/no-code platforms, GDPR compliance, and comparative studies, highlighting the research gap. Section 3 details the requirements analysis, including user personas, GDPR-derived requirements, and a benchmark chronic disease management application. Section 4 describes the system design and implementation in Mendix and OutSystems. Section 5 presents the evaluation methodology, findings, and both quantitative and qualitative results. Section 6 discusses implications, positioning the findings within the broader literature and noting limitations. Section 7 concludes and outlines directions for future work.

2 BACKGROUND AND RELATED WORK

Model-based software engineering (MBSE) techniques emphasise the central role of models in the analysis, design, and implementation of systems. Low-code/no-code (LCNC) platforms represent a form of model-driven development where applications are constructed through visual models, predefined components, and configuration rather than traditional coding. These environments are increasingly used across sectors to accelerate digital transformation and reduce reliance on scarce IT resources (Sanchis et al., 2019) (Luo et al., 2021).

2.1 Low-Code/No-Code Platforms as Model-Based Environment

Low-code/no-code (LCNC) platforms extend the principles of model-driven development to non-technical users, sometimes referred to as "citizen developers." Using visual modelling notations, templates, and drag-and-drop interfaces, platforms such as Mendix and OutSystems enable rapid prototyping of applications without deep programming knowledge (Richardson and Rymer, 2014; Beranič et al., 2020). Gartner (Gartner, 2021) reports that LCNC approaches can reduce development times by up to 90% compared to traditional methods. In practice, this represents a shift towards domain-specific modelling, where end-users directly encode their expertise into application logic (Luo et al., 2021; Rokis and Kirikova, 2023).

In healthcare, this potential is significant. Clinicians and researchers often need bespoke applications for monitoring, consent management, or patient engagement, but lack the programming expertise required for traditional development. LCNC platforms promise to bridge this gap by allowing medical professionals to model workflows and deploy functional prototypes that align closely with their domain needs (Sanchis et al., 2019; Ferreira et al., 2019; Alsaadi et al., 2021).

2.2 GDPR Compliance in Model-Based Development

This study focuses on five GDPR provisions (Articles 5, 6, 7, 25, and 32) that can be directly operationalised within low-code/no-code (LCNC) platforms by non-technical users. In healthcare, personal data constitute "special category data," requiring enhanced protection under the GDPR (European Union, 2016). These provisions were selected as both *critical* for compliance and *actionable* at the application level, whereas organisational responsibilities (e.g., contractual obligations or data protection officers) fall outside the scope of application builders.

Article 5 – Personal data must be limited to defined purposes and necessity, with appropriate retention and protection against unauthorised access or modification (European Union, 2016), and reflected in healthcare data models, forms, and workflows.

Article 6 – Lawfulness of processing. Processing is lawful only where a valid legal basis applies—typically healthcare provision or explicit consent for secondary use—and must be documented within the application (European Union, 2016).

Article 7 – Conditions for consent. Consent must be informed, specific, unambiguous, and withdrawable, with evidence of capture and withdrawal (European Union, 2016). This requires explicit consent

management support, which many health applications lack (Fan et al., 2020).

Article 25 – Data protection by design and by default. Only personal data necessary for each purpose should be processed by default (European Union, 2016), making privacy-preserving defaults essential in LCNC platforms used by non-technical professionals (Hussain et al., 2018).

Article 32 – Security of processing. Security measures proportionate to risk, including encryption, access control, and audit logging, are required (European Union, 2016), yet studies report gaps in healthcare systems' ability to enforce and evidence them (Fan et al., 2020; Hussain et al., 2018; Cummins et al., 2020).

Overall, these five provisions capture the *application-level compliance capabilities* that can realistically be implemented by non-technical domain experts, making them suitable criteria for evaluating LCNC platforms in GDPR-regulated healthcare contexts.

2.3 Prior Comparative Studies

Comparative analyses of LCNC platforms typically focus on productivity, usability, and integration capabilities (Alsaadi et al., 2021; Rokis and Kirikova, 2023). However, there is limited empirical evidence on their compliance readiness, especially in regulated domains. OutSystems has been adopted in healthcare projects such as NHS mobile services and Promedico medication management systems, while Mendix has been applied in clinical prototyping with support for domain experts through its "Studio" environment. Both platforms support enterprise security standards (ISO, HIPAA, GDPR), yet the accessibility of these features for non-technical users has not been systematically evaluated.

Beyond LCNC comparisons, related work has examined GDPR compliance through model-driven methods. Torre et al. (Torre et al., 2020) applied model-driven engineering to formalise GDPR requirements using UML models and OCL constraints, highlighting the role of traceability in regulatory compliance. Vanezi et al. (Vanezi et al., 2024) proposed an approach to incorporate GDPR purpose limitation into requirements analysis, providing early design guidance. Galhardo and Silva (Galhardo and Silva, 2022) investigated the integration of rigorous requirements specifications with a low-code platform (Genio), showing trade-offs between formal modelling and low-code implementation. While these studies contribute important insights, they do not assess how commercial LCNC platforms expose GDPR features to non-technical users, which is the focus of this paper.

2.4 Research Gap

Although LCNC platforms represent a model-based approach to application development, their role in enabling GDPR compliance for non-technical medical professionals is underexplored. Most studies focus on technical capabilities or productivity benefits, leaving unanswered whether compliance-relevant modelling tasks can be achieved by citizen developers without extensive developer intervention. This study addresses this gap by presenting a requirements-driven, model-based evaluation of Mendix and OutSystems, using GDPR articles as measurable criteria.

3 REQUIREMENTS ANALYSIS

Requirements analysis provides the foundation for evaluating whether low-code/no-code (LCNC) platforms can support the development of GDPR-compliant healthcare applications by non-technical medical professionals. In this study, GDPR provisions were operationalised into concrete modelling requirements, instantiated in a benchmark application, and evaluated through systematic metrics.

3.1 User Personas

Following best practice in requirements engineering, personas were defined to approximate the experience of non-technical medical professionals. Personas are widely recognised as a user-centred technique for clarifying requirements and representing archetypical users in software projects (Ferreira et al., 2018; Karolita et al., 2023). In health informatics, personas have been shown to improve stakeholder engagement and ensure that applications are aligned with end-user needs (Bhattacharyya et al., 2019; Schäfer et al., 2019).

As shown in Figure 1, one of these personas for a clinical researcher is presented. Further personas are described in the publicly accessible dissertation documents available at (Obiora, 2025, p. 31). The personas guided all evaluation tasks, constraining implementation choices to features discoverable through modelling and configuration. Three personas—a doctor, nurse, and clinical researcher—were introduced. All personas combine domain expertise with limited technical skills, ensuring the study reflects the

Figure 1: User persona for a clinical researcher representing non-technical medical professionals used in the evaluation.

constraints non-technical users face when building GDPR-compliant applications in LCNC platforms.

3.2 Platform Considerations

LCNC platforms were selected based on their prominence in both industry and academia (Mendix and OutSystems) and their alignment with critical criteria for healthcare app development:

- **Security and Compliance**: enterprise-grade security, encryption, and role-based access control (Knorr and Aspinall, 2015; Hussain et al., 2018).
- **GDPR Alignment**: capacity to configure workflows aligned with Articles 5, 6, 7, 25, and 32 of the GDPR (European Union, 2016).
- **Ease of Implementation**: intuitive visual interfaces enabling non-technical users to configure forms, workflows, and access rules (Beranič et al., 2020; Mohammadkhani et al., 2025).

These considerations reflect the literature indicating that security and compliance remain primary challenges in mobile health app development (Fan et al., 2020; Cummins et al., 2020).

3.3 GDPR-Derived Requirements

Five GDPR provisions (Articles 5, 6, 7, 25, and 32) were operationalised into concrete modelling requirements for the benchmark application, covering data minimisation, lawful processing, consent capture and withdrawal, privacy by design/default, and secure processing with encryption and audit trails.

3.4 Benchmark Application Features

A benchmark *chronic disease management application* was specified to instantiate the requirements. Its core features included:

- **User registration and authentication** with role-based access (Articles 25, 32).
- **Personal and medical information screens** limited to clinically relevant attributes (Article 5).
- **Consent capture and withdrawal**, including a privacy policy screen and account deletion workflows (Articles 6, 7).
- **Emergency contact and monitoring features**, restricted to essential data fields (Articles 5, 25).
- **Settings and audit logs** providing visibility of consent withdrawal and account deletion events (Articles 7, 32).

These features were informed by literature on effective chronic disease management applications (Mao et al., 2020; Serrano et al., 2023; Kim et al., 2025).

3.5 Evaluation Metrics

Each requirement was linked to an evaluation metric to capture both platform capability and user accessibility:

- **Support**: whether the feature exists natively in the platform.
- **Ease of Implementation**: the effort required for a non-technical user to configure the feature.
- **Auditability**: whether the platform provides compliance evidence, such as logs of consent or access events.
- **Cost/Tier**: whether the feature is available in free tiers or requires enterprise licensing.

These metrics were combined into a Compliance Implementation Score (CIS), extending existing LCNC evaluation frameworks (Rokis and Kirikova, 2023; Alsaadi et al., 2021) to the GDPR compliance context.

4 SYSTEM DESIGN AND IMPLEMENTATION

The evaluation required the development of a benchmark *chronic disease management application* in both Mendix and OutSystems. The prototypes were designed under the assumption of a non-technical medical professional persona (doctor, nurse, researcher), thus constraining implementation choices to platform-native modelling constructs such as visual forms, logic flows, and access control settings.

4.1 Prototype Overview

The benchmark application included user registration and authentication, patient profile creation, consent

capture and withdrawal, symptom monitoring, and account deletion features. These functionalities were chosen because they map directly to the GDPR requirements described in Section 3.

- **User registration and authentication**: Implemented using built-in account creation modules with secure password handling and role-based access.
- **Patient profile management**: Enabled entry of essential demographic and clinical data fields, constrained to the minimum required attributes (GDPR Article 5).
- **Consent management**: Configured through privacy policy screens, toggle-based consent options, and workflows linking consent withdrawal to account deletion (GDPR Articles 6 and 7).
- **Symptom monitoring**: Created as forms and dashboards for recording clinical symptoms, restricted by role-based permissions (GDPR Articles 5 and 25).
- **Account deletion and audit**: Linked to consent withdrawal and deletion workflows, leaving an audit trace of actions performed (GDPR Articles 7 and 32).

4.2 Mendix Implementation

Mendix Studio provided a highly visual modelling environment, where pages and workflows were defined through drag-and-drop components. Privacy-by-default was supported by configuring role-based access at the entity level. Consent capture was implemented using a native "page flow" template, while consent withdrawal was linked to account deletion via a microflow. Security features such as HTTPS encryption and secure authentication were enforced by default. However, full auditability of consent changes required additional configuration through marketplace modules.

4.3 OutSystems Implementation

OutSystems Service Studio enabled similar functionality through reusable templates and workflow diagrams. While more flexible in terms of UI design and custom workflows, many GDPR features required greater configuration effort. For example, data minimisation required explicit schema editing, while privacy-by-default demanded careful assignment of roles and permissions to each page. Consent management workflows could be modelled but required additional logic to link to account deletion. OutSystems offered strong enterprise features, but these were often tied to paid tiers, making them less accessible to non-technical users working in free versions.

4.4 Evidence Collection

Implementation in both platforms was documented using annotated screenshots, workflow logs, and time-on-task measurements. These artefacts provided evidence for scoring against the evaluation metrics of Support, Ease of Implementation, and Auditability. The combination of these artefacts produced a traceable evaluation process linking GDPR requirements to platform capabilities, in line with model-based evaluation principles (Beranič et al., 2020; Rokis and Kirikova, 2023).

5 EVALUATION

The prototypes were evaluated against the GDPR-derived requirements (Section 3) using three main metrics: *Support*, *Ease of Implementation*, and *Auditability*. A fourth contextual metric, *Cost/Tier*, was also noted to capture whether compliance-relevant features were available in free tiers or restricted to enterprise licensing. A detailed account of the evaluation is presented in the relevant dissertation chapter (Obiora, 2025).

5.1 Evaluation Methodology

Each GDPR article was operationalised into specific modelling tasks within the benchmark application. For example, Article 7 (Consent) was tested by creating a privacy policy screen, capturing explicit opt-in consent, and linking consent withdrawal to account deletion workflows. Tasks were performed separately in Mendix and OutSystems under the constraint of the non-technical medical professional persona. Implementation time, number of configuration steps, and reliance on external modules were recorded. Evidence was collected through annotated screenshots, workflow logs, and configuration reports.

Each task was scored across the three core metrics:

- **Support** – whether the platform natively supported the requirement without custom coding.
- **Ease of Implementation** – the perceived difficulty for a non-technical user, measured by number of steps and intuitiveness of configuration.
- **Auditability** – whether compliance evidence (e.g., consent logs, access history) could be generated.

Scores were aggregated into a Compliance Implementation Score (CIS), extending comparative frameworks in the LCNC literature (Alsaadi et al., 2021; Rokis and Kirikova, 2023).

5.2 Findings

Results indicate that both Mendix and OutSystems provide strong baseline GDPR support, particularly for security of processing (Article 32). However, significant differences emerged in accessibility:

- **Mendix** – proved more user-friendly for consent management (Article 7). The prvacy-by-deafault (Article 25) was the same in both tools. Role-based access control could be configured visually, and consent workflows were relatively straightforward to implement. Audit logs required additional configuration but were partially available through marketplace modules.
- **OutSystems** – offered greater flexibility in data schema design and custom workflows, making it strong for data minimisation (Article 5). However, consent management and privacy-by-default required more complex configuration, often beyond the reach of a non-technical persona. Several compliance features were only accessible in enterprise tiers.

Figure 2 illustrates how Article 7 was instantiated, highlighting differences in accessibility. In Mendix (left), consent capture and withdrawal could be configured through a page-flow template with relatively few steps, making it accessible to non-technical users. In contrast, OutSystems (right) required additional workflow logic and role assignments to achieve the same functionality, increasing configuration effort. This comparison highlights a key trade-off identified by the evaluation framework: Mendix supports more intuitive consent workflows, while OutSystems provides greater flexibility but at higher complexity.

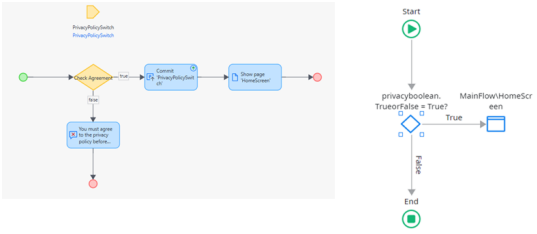

Figure 2: Consent workflow implementation in Mendix (left) and OutSystems (right), illustrating differences in accessibility for non-technical users when configuring GDPR Article 7 compliance.

5.3 Quantitative Summary

Figure 3 presents the central quantitative result of this study, illustrating how the Compliance Implementation Score (CIS) reveals trade-offs between ease of implementation in Mendix and fine-grained flexibility in OutSystems.

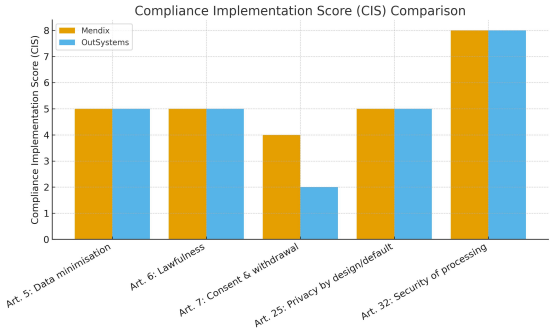

Figure 3: Compliance Implementation Score (CIS) comparison of Mendix and OutSystems across GDPR Articles 5, 6, 7, 25, and 32.

Across the GDPR articles, Mendix achieved consistently higher scores in Ease of Implementation, while OutSystems performed better in fine-grained control but lower in accessibility. Neither platform provided full native support for audit trails without additional configuration, limiting compliance evidence for Articles 7 and 32.

5.4 Qualitative Observations

Participants simulating the user personas reported that Mendix offered a smoother modelling experience, while OutSystems provided stronger enterprise-grade flexibility but required more technical knowledge. This confirms observations in the literature that usability and compliance are often in tension within LCNC platforms (Beranič et al., 2020; Fan et al., 2020). Mendix's simplicity may better serve non-technical medical professionals, while OutSystems may be preferable in hybrid teams with IT support.

6 DISCUSSION

The comparative evaluation of Mendix and OutSystems highlights the opportunities and limitations of low-code/no-code (LCNC) platforms as model-based environments for GDPR-compliant healthcare applications. While both platforms support baseline compliance requirements, significant differences emerged in terms of accessibility for non-technical

users, trade-offs between usability and flexibility, and the degree of compliance evidence available.

6.1 Usability versus Flexibility

Mendix consistently offered smoother workflows for GDPR-related tasks, particularly for consent capture (Article 7) and privacy-by-default (Article 25). These findings suggest that Mendix's design orientation toward non-technical "citizen developers" aligns with the needs of medical professionals seeking to model compliant workflows quickly. OutSystems, by contrast, provided more granular control over data models and workflows, making it stronger for data minimisation (Article 5) but less intuitive overall. This reflects a broader trade-off observed in LCNC literature between accessibility and fine-grained flexibility (Beranič et al., 2020; Rokis and Kirikova, 2023).

6.2 Compliance Evidence and Auditability

Neither platform provided complete support for generating compliance evidence without additional configuration. While encryption and secure authentication (Article 32) were enforced by default, audit trails for consent withdrawal and access control changes were only partially available. Marketplace modules and enterprise-tier features were often required to achieve full auditability. This confirms earlier findings that many digital health applications struggle with privacy and security compliance despite vendor claims (Fan et al., 2020; Hussain et al., 2018).

6.3 Implications and Positioning

From a model-based software engineering perspective, this study illustrates how regulatory requirements can be operationalised into modelling tasks and systematically evaluated across platforms. The results highlight that LCNC platforms lower the barrier to entry for non-technical professionals but do not remove the need for IT support in regulated domains. For healthcare organisations, this implies a hybrid development model where medical professionals can prototype GDPR-compliant workflows, while technical experts ensure robustness and auditability. These findings align with prior studies emphasising the potential of LCNC platforms for rapid prototyping in healthcare (Sanchis et al., 2019; Ferreira et al., 2019), while extending the literature by focusing explicitly on GDPR compliance. Unlike vendor white papers claiming "compliance by design" (Mendix, 2020; OutSystems, 2021), our results show that non-technical users still face challenges in evidencing compliance. This underscores the importance of evaluation frameworks that systematically link legal requirements to platform modelling capabilities.

6.4 Limitations

This study has several limitations. First, the evaluation simulated non-technical personas rather than involving medical professionals, which may affect external validity. Second, the benchmark application focused on chronic disease management and may not reflect the full range of healthcare contexts. Third, auditability was only partially tested due to licensing restrictions, so results may underestimate enterprise-level compliance support. Future work should address these issues through participatory evaluation and expanded test cases.

7 Conclusions and Future Work

This paper introduced a requirements-driven evaluation framework that operationalises five GDPR provisions—data minimisation (Art. 5), lawfulness of processing (Art. 6), consent (Art. 7), privacy by design and default (Art. 25), and security of processing (Art. 32)—into modelling tasks suitable for low-code/no-code (LCNC) environments. The framework was illustrated through a comparative case study of Mendix and OutSystems, using a benchmark chronic disease management application.

The study shows that both platforms provide baseline security and compliance features such as encryption and role-based access. However, differences in accessibility emerged: Mendix offers more intuitive workflows for consent and privacy-by-default, while OutSystems provides greater flexibility in schema design at the cost of higher configuration effort. Neither platform, however, provides complete auditability without additional modules or enterprise licensing.

These findings demonstrate that LCNC platforms can lower the barrier for non-technical medical professionals to develop GDPR-aware applications, but cannot ensure full compliance without technical oversight. The proposed evaluation framework provides a structured way to assess compliance support in model-based platforms and can guide both researchers and practitioners in selecting LCNC tools for regulated healthcare contexts.

Future work should involve participatory evaluation with medical professionals, extend the framework to additional GDPR provisions such as data

portability and the right to object, and assess interoperability with clinical systems. Expanding the comparative scope to include other LCNC platforms will further validate the generality of the framework.

REFERENCES

Alsaadi, I., Alsadi, A., and Ahmad, A. (2021). A comparative study of low-code development platform. *International Journal of Advanced Computer Science and Applications*, 12(5):256–263.

Beranič, T., Heričko, M., and Rozman, I. (2020). Low-Code Development Platforms: A Systematic Mapping Study. *Computer Standards & Interfaces*, 72:103451.

Bhattacharyya, O., Mossman, K., Gustafsson, L., and Schneider, E. C. (2019). Using Human-Centered Design to Build a Digital Health Tool: Personae and Prototypes. *Journal of Medical Internet Research*, 21(5):e10318.

Cummins, N., Schuller, B., Kächele, M., Stasak, B., and Cowie, R. (2020). Privacy and Security Considerations for Mobile Health Systems. *IEEE Internet Computing*, 24(2):29–37.

European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016: General Data Protection Regulation. Official Journal of the European Union, L119, 1–88.

Fan, Y., Zhang, X., and Sun, J. (2020). Privacy risks of mobile health apps: A systematic review. *Telemedicine and e-Health*, 26(10):1314–1321.

Ferreira, A., Correia, A., and Silva, A. R. (2019). OutSystems in Healthcare: A Case Study of Mobile Health Applications for the Portuguese NHS. In *Procedia Computer Science*, volume 164, pages 523–530.

Ferreira, B., Sharp, H., Robinson, H., and Budgen, D. (2018). A Technique for Representing Requirements Using Personas: A Controlled Experiment. *IET Software*, 12(5):280–292.

Galhardo, I. and Silva, A. (2022). Combining Rigorous Requirements Specifications with Low-Code Platforms to Rapidly Develop Business Applications. *Applied Sciences*, 12(19):9556.

Gartner (2021). Magic Quadrant for Enterprise Low-Code Application Platforms. Gartner Research.

Hussain, M., Abou-Tair, D., and Abou-Tair, M. (2018). Security and Privacy in Mobile Health Applications: A Review. *Journal of Medical Systems*, 42(5):88.

Karolita, D., Kanij, T., Grundy, J., McIntosh, J., and Obie, H. O. (2023). Use of Personas in Requirements Engineering: A Systematic Literature Review. *Information and Software Technology*, 157:107264.

Kim, S., Park, H., and Lee, J. (2025). Requirements-Driven Design of Health Monitoring Apps: A GDPR Perspective. *Journal of Biomedical Informatics*, 146:104479.

Knorr, K. and Aspinall, D. (2015). Security and Usability in Health IT: A Case Study of Access Control Requirements. In *Proceedings of the 2015 ACM Conference on Computer Security*, pages 123–134.

Luo, J., Reddi, V., and Zhang, H. (2021). Low-code/no-code development platforms: Opportunities, challenges, and directions. *IEEE Software*, 38(4):40–47.

Mao, Y., Chen, Y., Wang, X., and Xu, C. (2020). Mobile Health Apps for Chronic Disease Management: A Review of Features and Functionality. *JMIR mHealth and uHealth*, 8(9):e16892.

Mendix (2020). Building GDPR-compliant apps with Mendix. `https://www.mendix.com/`.

Mendix (2025). Mendix: Low-Code Application Development Platform. `https://www.mendix.com/`. Accessed: 16 September 2025.

Mohammadkhani, R., Ghasemi, M., and Rahmani, A. M. (2025). Low-Code Development in Healthcare: Usability and Security Challenges. *Information Systems Frontiers*.

Obiora, C. (2025). Comparative Analysis of Low-Code/No-Code Development Platforms for the Development of Health Applications by Non-Technical Medical Professionals.

OutSystems (2021). NHS mobile apps built with OutSystems: Enhancing patient engagement and staff productivity. `https://www.outsystems.com/`.

OutSystems (2025). OutSystems: High-Performance Low-Code Platform. `https://www.outsystems.com/`. Accessed: 16 September 2025.

Richardson, C. and Rymer, J. (2014). New Development Platforms Emerge for Customer-Facing Applications. Technical report, Forrester Research.

Rokis, K. and Kirikova, M. (2023). Selecting low-code platforms: Evaluation framework and case study, journal = Information Systems and e-Business Management. 21(1):67–88.

Sanchis, R., García-Peñalvo, F. J., and Fombona, J. (2019). Low-Code as Enabler of Digital Transformation in Education and Healthcare. *IEEE Access*, 7:150150–150159.

Schäfer, K., Diefenbach, S., and Hassenzahl, M. (2019). Survey-based Personas for a Target-Group-Specific Approach in Medical Technology Systems. *International Journal of Medical Informatics*, 128:18–25.

Serrano, J. C., Martins, H., and Silva, T. (2023). Evaluating Mobile Applications for Patient Self-Management of Chronic Illness. *International Journal of Medical Informatics*, 170:104991.

Torre, D. D., Micucci, D., and Mariani, L. (2020). Model Driven Engineering for Data Protection and Privacy: Application and Experience with GDPR. In *Proceedings of the 2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*, pages 133–136.

Vanezi, M., Kapitsaki, G., and Philippou, A. (2024). What's Your Purpose? An Approach to Incorporating GDPR Purposes into Requirements Analysis. In *Proceedings of the 12th International Conference on Model-Driven Engineering and Software Development (MODELSWARD)*, pages 141–152. SCITEPRESS.