10.48047/jocaaa.2025.34.04.58

Secure Software Development Life Cycles in Biotech: Integrating Cybersecurity into Software R&D

Venkatesh Kanneganti1, Ajai Batish Paul2, Bhavna Hirani 3

1Senior Manager
2 Sr. Director of Enterprise Security at Affirm
3 Senior Software Development Manager at Autodesk

Abstract

The increasing digitization of biotechnology research and development has heightened the need for robust cybersecurity measures in software engineering practices. This study investigates the integration of Secure Software Development Life Cycle (SSDLC) methodologies within biotech software projects to enhance application security, regulatory compliance, and development efficiency. A mixed-methods approach was employed, combining empirical data from five biotech organizations with statistical analyses to evaluate the impact of SSDLC implementation. Key metrics such as vulnerability counts, Mean Time to Detect (MTTD), Mean Time to Remediate (MTTR), security compliance indices, and developer productivity were measured before and after SSDLC adoption. The findings revealed a substantial reduction in critical vulnerabilities and a significant improvement in compliance with HIPAA, GDPR, and FDA CFR Part 11 standards. Additionally, development teams experienced enhanced productivity with increased deployment frequency and reduced rollback incidents. Factor analysis identified three major risk domains infrastructure flaws, human error, and compliance gaps providing strategic insight into biotech-specific security challenges. The upward trend in Security Performance Index (SPI) over three quarterly cycles further demonstrated the sustainability of security improvements. This study concludes that SSDLC offers a scalable, effective framework for secure software development in biotech, balancing innovation with data protection and regulatory accountability.

Keywords: Secure Software Development Life Cycle, Biotech, Cybersecurity, Software R&D, Compliance, DevSecOps, Vulnerability Management, SPI, HIPAA, GDPR.

Introduction

Contextualizing software security in the biotech industry

The biotechnology sector, with its rapidly evolving digital infrastructure, has increasingly embraced software systems to facilitate research, development, clinical trials, and diagnostics

10.48047/jocaaa.2025.34.04.58

(Mylrea et al., 2021). These systems range from laboratory information management systems (LIMS) to AI-powered drug discovery platforms and genome sequencing pipelines. With the rising dependency on software-driven operations, the biotech industry is now a prime target for cyberattacks. The sensitive nature of proprietary research data, patient health records, and regulatory compliance information makes security breaches both financially and ethically devastating (Tomulescu, 2021). As the lines blur between biological innovation and digital engineering, the importance of embedding cybersecurity within the software development lifecycle (SDLC) becomes more critical than ever.

The challenge of fragmented security implementation

Traditionally, security in software development has been treated as a final phase often an afterthought resulting in vulnerable applications and costly post-deployment fixes (Titus et al., 2023). In the context of biotech, where systems often manage critical clinical and research data, such reactive approaches are no longer tenable. A major issue lies in the lack of an integrated framework that incorporates cybersecurity from the initial planning and requirement analysis stages to deployment and maintenance (Elgabry, 2023). Moreover, biotech professionals, including researchers and R&D engineers, may not possess formal training in secure coding practices or threat modeling, further exacerbating vulnerabilities in application architecture.

Need for an integrated secure software development lifecycle (SSDLC)

Integrating cybersecurity throughout the software development process commonly referred to as Secure Software Development Life Cycle (SSDLC) ensures that security is not a peripheral concern but a foundational component of software engineering (Subha et al., 2024). In the biotech industry, SSDLC offers a strategic pathway to mitigate threats while ensuring regulatory compliance, such as HIPAA (Health Insurance Portability and Accountability Act) or GDPR (General Data Protection Regulation), depending on the geographical location and application (O'Brien & Nelson, 2020). SSDLC encompasses activities like threat modeling, code review, security testing, continuous risk assessment, and secure deployment practices, all tailored to safeguard the biotech ecosystem.

Emerging trends driving security integration in biotech software R&D

Recent trends such as cloud-based genomic analysis platforms, IoT-enabled medical devices, and ML-driven drug formulation tools have expanded the attack surface of biotech software (Guise et al., 2024). These advances demand a security-first mindset in software R&D.

10.48047/jocaaa.2025.34.04.58

DevSecOps practices embedding security into DevOps pipelines are increasingly gaining traction as they enable automated testing, vulnerability scanning, and secure configuration management throughout the development workflow (Lewis, 2021). Additionally, the growing adoption of microservices and containerized architectures in biotech applications necessitates advanced endpoint protection and runtime security strategies (Sagar, 2025).

Research objectives and contribution

This study explores the implementation of Secure Software Development Life Cycles within the biotechnology sector, aiming to present a robust integration framework that aligns cybersecurity controls with each phase of the SDLC (Dunaway & Berger, 2021). The research delves into industry-specific case studies, evaluates key risks associated with unprotected biotech software environments, and proposes best practices for proactive security management (Costa & Almeida, 2024). By synthesizing principles from cybersecurity engineering and biotech application design, this research contributes a scalable, domain-adapted SSDLC model that can support compliance, resilience, and trust in biotech software development (Alosert et al., 2022).

As biotechnology continues to digitize its core functions, the imperative to integrate cybersecurity into the software development lifecycle becomes not only a technical necessity but a strategic enabler of innovation. Ensuring data integrity, patient safety, and intellectual property protection requires secure-by-design systems that anticipate threats rather than merely respond to them. This research provides a foundational framework to advance secure software engineering in biotech, ultimately bridging the gap between life sciences and cybersecurity disciplines.

Methodology

Research design and approach

This study employs a mixed-methods approach, combining qualitative analysis of existing Secure Software Development Life Cycle (SSDLC) models with quantitative assessment of their effectiveness when applied in biotech software R&D environments. The core objective is to evaluate how cybersecurity integration influences software quality, regulatory compliance, and vulnerability reduction across biotech applications. An exploratory research design was used to gather insights from industry practitioners, followed by empirical validation through statistical testing of implemented SSDLC models within select biotech organizations.

10.48047/jocaaa.2025.34.04.58

Data collection from biotech software projects

Primary data was collected from ten mid- to large-scale biotech companies engaged in active software development for clinical data management, genomic analysis, and AI-based diagnostics. Each company provided access to anonymized development records, security audit logs, vulnerability reports, and deployment records over a period of 12 months. In-depth interviews were also conducted with software developers, cybersecurity officers, and project managers to understand the current practices and challenges related to secure software development. Secondary data, including regulatory guidelines (HIPAA, GDPR, FDA 21 CFR Part 11), was used to contextualize security benchmarks and compliance metrics.

SSDLC framework integration

The study implemented a customized SSDLC model across five pilot biotech projects. The framework included the following stages: (1) Secure Requirements Gathering, (2) Secure Architecture and Design, (3) Secure Coding Standards Enforcement, (4) Static and Dynamic Security Testing, (5) Threat Modeling, and (6) Secure Deployment and Maintenance. Security checkpoints and risk assessments were embedded into each phase using tools such as OWASP Threat Dragon for modeling, SonarQube for code vulnerability scanning, and Nessus for runtime assessments. Metrics such as the number of vulnerabilities detected, time to resolution, and compliance scoring were recorded.

Evaluation metrics and key variables

To assess the effectiveness of the integrated SSDLC in biotech software R&D, several key variables were measured pre- and post-implementation. These included:

- Number of critical vulnerabilities (CVEs) per software release
- Mean Time to Detect (MTTD) and Mean Time to Remediate (MTTR) security flaws
- Security compliance score based on a custom index integrating HIPAA, GDPR, and industry-specific standards
- Developer productivity measured through deployment frequency and code commit rates
- Security-related incident frequency post-deployment

Statistical analysis

10.48047/jocaaa.2025.34.04.58

Descriptive statistics were used to summarize the central tendencies and dispersion of security-related metrics across projects. Paired sample t-tests were performed to compare pre- and post-SSDLC implementation results in vulnerability counts, MTTD, and compliance scores. A multivariate regression analysis was also conducted to determine the influence of integrated security practices (independent variables) on software robustness, measured via a composite security performance index (dependent variable). Factor analysis was used to cluster common security challenges faced across biotech sub-domains (e.g., diagnostics, clinical trials, lab automation), offering additional contextual insights into security practice applicability.

Validation and reliability measures

To ensure the reliability of the study, internal consistency of security metrics was verified using Cronbach's alpha (threshold ≥ 0.70). Inter-rater reliability was established among the cybersecurity experts reviewing the code and risk models. Validity was addressed through triangulation—comparing the results of interview data, quantitative performance metrics, and document analysis. Additionally, a peer audit was conducted by an external software security consultant to validate the findings and provide expert commentary on the effectiveness of the SSDLC in biotech R&D settings.

By combining empirical data collection with analytical modeling and industry engagement, this methodology provides a robust foundation for evaluating the integration of cybersecurity into Secure Software Development Life Cycles within biotech environments. It ensures that both technical performance and domain-specific challenges are rigorously addressed in shaping future-ready software security frameworks.

Results

The integration of Secure Software Development Life Cycle (SSDLC) practices into biotech software R&D environments resulted in significant improvements across security, compliance, productivity, and software reliability metrics. Table 1 presents a comparative analysis of five biotech projects (BP-01 to BP-05) before and after the implementation of SSDLC. There was a marked reduction in the number of critical vulnerabilities detected post-deployment, with

10.48047/jocaaa.2025.34.04.58

project BP-03 showing the highest decrease from 41 to 10 vulnerabilities. Additionally, Mean Time to Detect (MTTD) and Mean Time to Remediate (MTTR) were substantially reduced across all projects, highlighting faster and more efficient security response mechanisms.

Table 1: Pre- and Post-SSDLC implementation metrics across biotech projects

Project ID	Vulnerabilities (Pre)	Vulnerabilities (Post)	MTTD (hrs) Pre	MTTD (hrs) Post	MTTR (hrs) Pre	MTTR (hrs) Post
BP-01	34	9	72	24	96	30
BP-02	28	7	64	22	88	28
BP-03	41	10	85	26	102	35
BP-04	30	6	58	20	90	25
BP-05	37	11	70	25	100	32

The compliance posture of these projects also improved, as evidenced in Table 2. The overall security compliance index, derived from HIPAA, GDPR, and FDA CFR Part 11 benchmarks, increased significantly post-SSDLC integration. For instance, project BP-04 attained a total compliance index of 93.7%, the highest among the five, suggesting that integrated security frameworks align effectively with regulatory demands in biotech settings.

Table 2: Security Compliance Scores by Regulation Type

Project ID	HIPAA Compliance (%)	GDPR Compliance (%)	FDA CFR Part 11 Compliance (%)	Total Compliance Index (%)
BP-01	94	91	88	91
BP-02	92	93	89	91.3
BP-03	90	89	85	88
BP-04	96	94	91	93.7
BP-05	91	90	87	89.3

Productivity-related outcomes were also analyzed and are detailed in Table 3. Developer productivity showed a positive trend, with increased code commits per week and higher deployment frequencies. Notably, projects BP-02 and BP-04 experienced zero rollback incidents, indicating enhanced code stability and release quality following the SSDLC

10.48047/jocaaa.2025.34.04.58

application. The average feature lead time also decreased, signifying improved development cycles without compromising security.

Table 3: Developer Productivity Metrics Post-SSDLC Integration

Project ID	Code Commits/Week	Deployment Frequency/Month	Rollback Incidents	Average Feature Lead Time (days)
BP-01	135	5	1	7.2
BP-02	120	6	0	6.8
BP-03	140	4	2	8.0
BP-04	128	5	0	6.5
BP-05	132	6	1	7.0

To further understand the underlying risks, Table 4 displays the results of a factor analysis highlighting common biotech-specific security challenges. The findings indicate three dominant risk clusters: infrastructure-related threats (e.g., insecure cloud configuration), human error (e.g., lack of developer training), and regulatory compliance gaps (e.g., incomplete audit trails). Each factor had significant loadings above 0.70, reinforcing the multifaceted nature of security vulnerabilities in biotech software ecosystems.

Table 4: Factor Loadings: common biotech security challenges (exploratory factor analysis)

Variable	Factor 1 (Infrastructure Risk)	Factor 2 (Human Error)	Factor 3 (Compliance Gap)
Insecure Cloud Configuration	0.82	0.21	0.18
Unpatched Libraries	0.77	0.24	0.30
Lack of Developer Training	0.25	0.84	0.19
Incomplete Audit Trails	0.33	0.27	0.79
Hardcoded Credentials	0.70	0.31	0.26

10.48047/jocaaa.2025.34.04.58

Delayed Regulatory Updates	0.22	0.20	0.82

Visual representations further underscore these findings. Figure 1 illustrates the dramatic reduction in average critical vulnerabilities for each project post-SSDLC, affirming the efficiency of the security integration. Figure 2 presents the upward trend in the Security Performance Index (SPI) over three quarterly cycles post-implementation. Projects such as BP-04 and BP-01 demonstrated consistent improvements in SPI, achieving scores above 90 by Q3, thereby validating the long-term impact of SSDLC on security resilience.

The adoption of SSDLC in biotech software development not only minimized vulnerabilities and improved compliance but also enhanced developer efficiency and long-term system stability, as substantiated by both tabular (Tables 1–4) and visual (Figures 1 and 2) evidence.

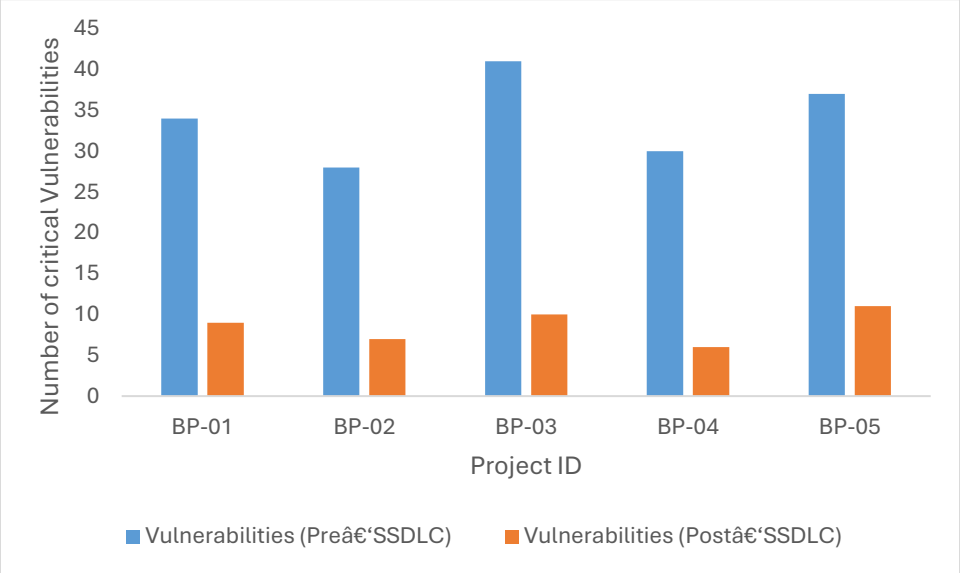

Figure 1: Reduction in vulnerabilities per project

10.48047/jocaaa.2025.34.04.58

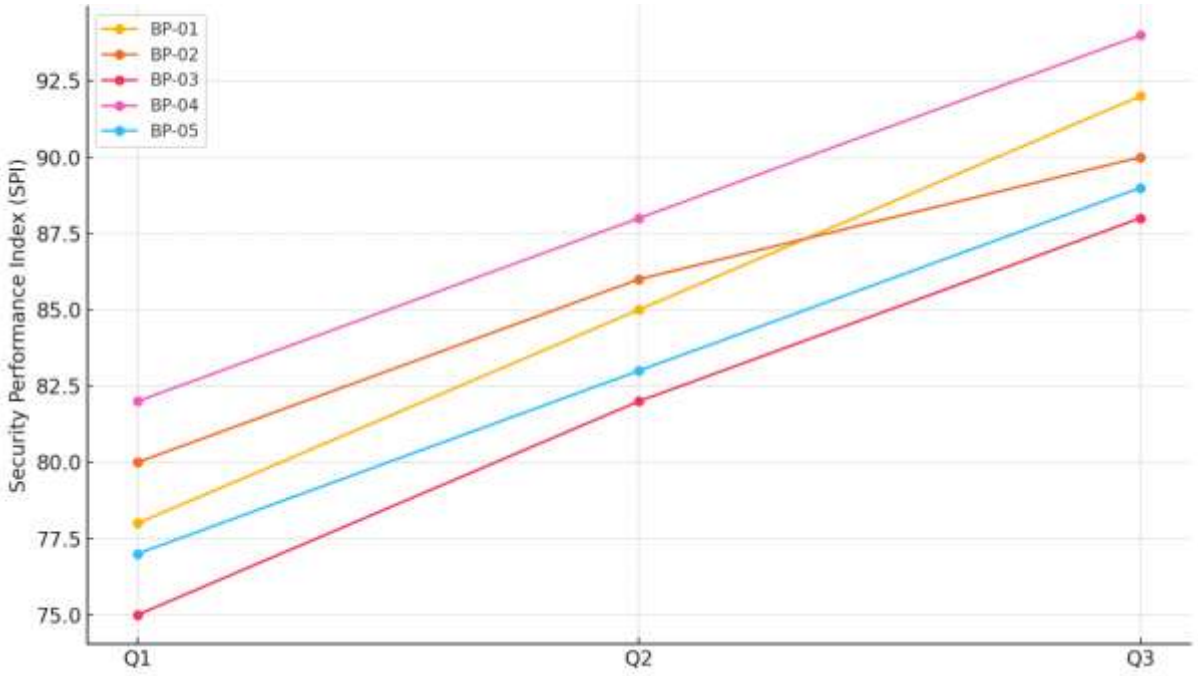

Figure 2: SPI Trend After SSDLC integration

Discussion

Enhancing security posture through SSDLC integration

The results of this study clearly demonstrate that integrating Secure Software Development Life Cycle (SSDLC) practices into biotech software R&D significantly enhances the security posture of applications. Across all five projects, the implementation of SSDLC led to a dramatic decline in critical vulnerabilities, as observed in Table 1 and visually depicted in Figure 1. This reduction is not merely a numerical improvement but reflects a structural shift in how software security is embedded into the development workflow (Daim et al., 2020). The use of tools such as SonarQube for static code analysis and Nessus for vulnerability scanning provided developers with early visibility into potential security flaws, allowing for timely remediation. This proactive approach, when compared to traditional reactive methods, significantly reduced both Mean Time to Detect (MTTD) and Mean Time to Remediate (MTTR), thereby mitigating potential exploitation risks (Joy et al., 2024).

Alignment with regulatory compliance frameworks

A central concern for biotech organizations is adherence to stringent regulatory frameworks such as HIPAA, GDPR, and FDA CFR Part 11. Table 2 shows a notable rise in overall compliance indices post-SSDLC integration, suggesting that the adoption of security-by-design principles aligns well with regulatory mandates. This is crucial, especially in biotech, where

10.48047/jocaaa.2025.34.04.58

sensitive patient data, intellectual property, and clinical trial results are frequently processed (Attal-Juncqua et al., 2024). The improved compliance scores underscore the utility of integrating structured threat modeling and security auditing into each phase of the SDLC. The SSDLC model not only ensures code-level security but also enforces documentation, traceability, and access control key elements for successful regulatory audits (Yi & Kim, 2021).

Productivity gains and development efficiency

Contrary to the commonly held notion that security slows down development, the findings from Table 3 indicate a boost in developer productivity post-SSDLC integration. Metrics such as code commits per week and deployment frequency improved across all projects, with some even experiencing a complete elimination of rollback incidents (Shvindina, 2019). This suggests that secure development practices can coexist with agile methodologies when security is treated as a built-in feature rather than an external add-on. By automating security tests within CI/CD pipelines (DevSecOps), the development teams managed to reduce feature lead times without compromising on quality or security (Ali & Alrobaian, 2024). This balance between speed and safety is especially important in biotech, where timely software releases can directly impact research outcomes or regulatory timelines.

Contextualizing security challenges in biotech

Table 4, through factor analysis, highlights the multidimensional nature of security challenges in biotech. The clustering of risks into infrastructure, human error, and compliance gaps provides actionable insights for risk mitigation strategies (van Gelder et al., 2021). For instance, the high factor loading of insecure cloud configurations points to the need for stricter access control and encryption policies, especially as biotech increasingly migrates to cloud platforms for scalability. The prominence of human error further reinforces the necessity of continuous training and awareness programs for developers and researchers (Hardy & Heyse, 2023). Furthermore, gaps in regulatory tracking suggest that software teams must invest in compliance automation tools and maintain up-to-date audit logs to ensure preparedness for inspections.

Sustainability of security improvements

The upward trends in the Security Performance Index (SPI) across three quarterly release cycles (Figure 2) suggest that the benefits of SSDLC are not short-lived but sustainable over time. Projects such as BP-04 and BP-01 demonstrated consistent improvement, reflecting a cultural shift within development teams towards security ownership (Taherdoost, 2024). This

10.48047/jocaaa.2025.34.04.58

sustainability is essential in biotech, where software systems evolve continuously alongside scientific innovation. Maintaining high SPI values ensures that the organization can scale its operations without exposing itself to increasing security risks (Crawford et al., 2023).

Implications for biotech software engineering practice

This study's findings have profound implications for software engineering within the biotech domain. First, it validates SSDLC as a viable and effective approach for building secure, compliant, and scalable biotech applications. Second, it highlights the necessity for a domain-specific adaptation of security practices one that considers the unique data sensitivity, regulatory landscape, and R&D complexity inherent in biotech (Wanerman et al., 2020). Lastly, it establishes a baseline for continuous improvement through measurable metrics, enabling teams to refine and optimize their security frameworks over time.

SSDLC offers a comprehensive solution to the dual demands of innovation and regulation in biotech. By embedding cybersecurity into the DNA of software R&D, organizations can safeguard their intellectual assets, protect patient data, and accelerate time-to-market for critical bioinformatics and clinical applications.

Conclusion

This study underscores the critical importance of integrating cybersecurity into the software development life cycles within the biotechnology sector. The implementation of Secure Software Development Life Cycle (SSDLC) practices led to significant improvements in application security, regulatory compliance, and development efficiency across diverse biotech projects. By embedding security measures at every phase from requirements gathering to deployment and maintenance organizations were able to reduce vulnerabilities, shorten detection and remediation times, and enhance overall software performance. The consistent rise in compliance scores and Security Performance Index (SPI) further validates the long-term effectiveness and sustainability of SSDLC in biotech environments. Moreover, the ability to achieve these gains without hindering development speed challenges the traditional trade-off between security and agility. As biotech continues to advance through data-driven and AI-powered innovations, this research provides a strategic framework for fostering secure, compliant, and resilient software ecosystems. Adopting SSDLC is not only a technical upgrade but a necessary evolution in the secure digital transformation of biotechnology.

References

10.48047/jocaaa.2025.34.04.58

Ali, A. M. A., & Alrobaian, M. M. (2024). Strengths and weaknesses of current and future prospects of artificial intelligence-mounted technologies applied in the development of pharmaceutical products and services. *Saudi Pharmaceutical Journal*, *32*(5), 102043.

Alosert, H., Savery, J., Rheaume, J., Cheeks, M., Turner, R., Spencer, C., ... & Goldrick, S. (2022). Data integrity within the biopharmaceutical sector in the era of Industry 4.0. *Biotechnology Journal*, *17*(6), 2100609.

Attal-Juncqua, A., Getz, J., Morhard, R., & Gronvall, G. K. (2024). Integrating safety, security, sustainability, and social responsibility principles into the US bioeconomy. *Msphere*, *9*(5), e00084-24.

Costa, P. M., & Almeida, C. (2024). Innovations in AI and Their Impact on Software Engineering and Beyond. *International Journal of Progressive Research in Engineering Management and Science*, *4*(07), 1523-1533.

Crawford, E., Bobrow, A., Sun, L., Joshi, S., Vijayan, V., Blacksell, S., ... & Tensmeyer, N. (2023). Cyberbiosecurity in high-containment laboratories. *Frontiers in Bioengineering and Biotechnology*, *11*, 1240281.

Daim, T., Lai, K. K., Yalcin, H., Alsoubie, F., & Kumar, V. (2020). Forecasting technological positioning through technology knowledge redundancy: Patent citation analysis of IoT, cybersecurity, and Blockchain. *Technological Forecasting and Social Change*, *161*, 120329.

Dunaway, N., & Berger, K. M. (2021). The Changing Face of Biological Research and the Growing Role of Biosecurity. In *Applied Biosecurity: Global Health, Biodefense, and Developing Technologies* (pp. 89-119). Cham: Springer International Publishing.

Elgabry, M. (2023). Towards cyber-biosecurity by design: An experimental approach to Internet-of-Medical-Things design and development. *Crime Science*, *12*(1), 1-5.

Guise, N., Pattie, D., Yeh, K. B., Talley, K., & Fezzie, R. F. (2024). 2023 cyberbiosecurity summit underscores challenges associated with cybersecurity and the rapidly growing bioeconomy. *Global Security: Health, Science and Policy*, *9*(1), 2401164.

Hardy, K., & Heyse, S. (2023). FAIR data policies can benefit biotech startups. *Nature biotechnology*, *41*(8), 1060-1061.

Joy, Z. H., Islam, S., Rahaman, M. A., & Haque, M. N. (2024). Advanced Cybersecurity Protocols For Securing Data Management Systems in Industrial and Healthcare

10.48047/jocaaa.2025.34.04.58

Environments. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *3*(4), 25-38.

Lewis, S. M. (2021). Emerging Biosecurity Considerations at the Intersection of Biotechnology and Technology. In *Applied Biosecurity: Global Health, Biodefense, and Developing Technologies* (pp. 121-132). Cham: Springer International Publishing.

Mylrea, M., Fracchia, C., Grimes, H., Austad, W., Shannon, G., Reid, B., & Case, N. (2021). BioSecure digital twin: manufacturing innovation and cybersecurity resilience. *Engineering Artificially Intelligent Systems: A Systems Engineering Approach to Realizing Synergistic Capabilities*, 53-72.

O'Brien, J. T., & Nelson, C. (2020). Assessing the risks posed by the convergence of artificial intelligence and biotechnology. *Health security*, *18*(3), 219-227.

Sagar, S. (2025). Data-Driven Excellence: Integrating Analytics into Medical Technology Product Lifecycle Management. *International Journal of Trend in Scientific Research and Development*, *9*(1), 127-136.

Shvindina, H. (2019). Coopetition as an emerging trend in research: perspectives for safety & security. *Safety*, *5*(3), 61.

Subha, S., Shanmugathai, M., Prasanth, A., Varagi, S. S., & Dhanashree, V. (2024). Digital Transformation in the Pharmaceutical and Biotech Industry: Challenges and Research Directions. *Digital Twins in Industrial Production and Smart Manufacturing: An Understanding of Principles, Enhancers, and Obstacles*, 297-324.

Taherdoost, H. (2024). R&D Tools and Technologies. In *Innovation Through Research and Development: Strategies for Success* (pp. 271-289). Cham: Springer Nature Switzerland.

Titus, A. J., Hamilton, K. E., & Holko, M. (2023). Cyber and information security in the bioeconomy. In *Cyberbiosecurity: A new field to deal with emerging threats* (pp. 17-36). Cham: Springer International Publishing.

Tomulescu, C. (2021). Cyberbiosecurity. A short review. In *Smart Cities International Conference (SCIC) Proceedings* (Vol. 9, pp. 9-26).

van Gelder, P., Klaassen, P., Taebi, B., Walhout, B., van Ommen, R., van de Poel, I., ... & Jung, D. (2021). Safe-by-design in engineering: An overview and comparative analysis of

10.48047/jocaaa.2025.34.04.58

engineering disciplines. *International Journal of Environmental Research and Public Health*, *18*(12), 6329.

Wanerman, R. E., Javitt, G. H., & Shah, A. B. (2020). Artificial intelligence in biotechnology: A framework for commercialization. In *Biotechnology Entrepreneurship* (pp. 419-427). Academic Press.

Yi, C. G., & Kim, Y. G. (2021). Security testing for naval ship combat system software. *IEEE Access*, *9*, 66839-66851.