

Analysis of the Impact of Strengthened Cybersecurity Regulations on the FDA 510(k) Medical Device Clearance Market

Chuelwon Lee^{1,*}

¹RAQA Team, HUINNO Co., Ltd., 13F, Yuhan Corp. Bldg., 74 Noryangjin-ro, Dongjak-gu, Seoul 06927, Republic of Korea

ARTICLE INFO.

Article history:

Received:

Revised:

Accepted:

Published Online:

Keywords:

Compliance burden, Premarket notification, Review time, Security by design, Software bill of materials

Type:

doi:

ABSTRACT

The rapid digitalization of healthcare via AI/ML software and connected devices, collectively known as the Internet of Medical Things (IoMT), introduces severe cybersecurity risks threatening patient safety. In response, the U.S. Food and Drug Administration (FDA) implemented a mandatory cybersecurity rule effective October 2023. This rule requires comprehensive documentation, including SBOMs and threat modeling, for all 510(k) premarket submissions. This coincided with the mandatory electronic submission system (eSTAR), creating contrasting effects: a compliance burden from increased documentation versus eSTAR's efficiency gains. This study analyzes 80,749 FDA 510(k) clearance decisions across 2,866 product codes from 2000 to 2025. The analysis revealed a statistically significant overall increase in the average 510(k) registration period of 20.92 days (5%-95% IQR-filtered; raw estimate 23.05 days; $p < 0.001$) after the rule's implementation, consistent with the regulatory burden of cybersecurity documentation outweighing eSTAR's efficiency gains. However, confounders (eSTAR's learning curve, post-pandemic dynamics) cannot be ruled out, and the difference fell to about 1 day when compared with 2021-2023 submissions. A product-code analysis (152 codes with sufficient data) showed heterogeneous effects: review times lengthened in 37 codes, including picture archiving and communication systems (LLZ; +65.6 days), shortened in 14 ($p < 0.05$), and did not change significantly for AI-based image processing software (QIH; -21.4 days; $p = 0.43$). These results suggest that the substantive quality of cybersecurity documentation may be an important determinant of the clearance timeline. This study offers an initial post-enforcement estimate; results depend on the comparison period.

© 2026 ISC. All rights reserved.

1 Introduction

The modern healthcare environment is undergoing a rapid digital transformation, driven by the

increased network connectivity of medical devices, the proliferation of AI/ML-based software, and the adoption of Remote Patient Monitoring (RPM) systems. While these advancements have innovatively improved the efficiency and accessibility of patient care, they have simultaneously exposed serious cybersecurity vulnerabilities [1]; the limited resources of connected devices make them susceptible to at-

* Corresponding author.

Email address: lcw@huinno.com

ISSN: 2008-2045 © 2026 ISC. All rights reserved.

tacks such as denial of service and reconnaissance [2]. In particular, cyberattacks on healthcare systems, such as ransomware, the breach of sensitive Personal Health Information (PHI), and exploitation of vulnerabilities in patient safety-critical devices like Infusion Pumps (FRN) [3], can cause physical harm and significant financial and legal risks. Addressing these risks requires robust security governance and verifiable technical implementation; however, the impact of new mandatory regulations on the market's response capacity remains unclear in the literature.

In response, the U.S. Food and Drug Administration (FDA) implemented a new mandatory cybersecurity rule starting October 1, 2023, based on the Consolidated Appropriations Act, 2023 [4]. This regulation mandates that medical device manufacturers submit detailed cybersecurity documentation, including Software Bill of Materials (SBOMs), threat modeling, and vulnerability management plans, when filing a 510(k) premarket notification [5]. This is considered one of the most significant changes in the history of medical device regulation [6].

This regulatory shift also coincided with the mandatory use of eSTAR (Electronic Submission Form), resulting in a complex impact on the medical device clearance market. From the FDA's perspective, eSTAR was expected to reduce early submission rejections (RTA) due to formal deficiencies and increase review efficiency (efficiency gains). However, the burden of creating new, complex cybersecurity documentation [5] could plausibly delay the 510(k) clearance process (compliance burden). The actual net effect on the market clearance period is therefore subject to significant debate.

While existing academic literature has debated the necessity and technical requirements of these new cybersecurity mandates, few studies have provided a quantitative, post-enforcement analysis utilizing long-term market data to assess the real-world outcome of these contrasting forces. This study aims to bridge this gap by quantitatively analyzing the actual impact of the FDA's mandatory cybersecurity rule (October 1, 2023) on the 510(k) clearance market. It seeks to compare the change in average registration duration pre- and post-regulation through long-term trend analysis, and to identify the heterogeneity of the regulatory impact through product code segmentation analysis to derive strategic implications for information security governance and policy.

The remainder of this paper is structured as follows: Section 2 reviews the existing literature on cybersecurity threats, regulatory efficiency, and AI/ML governance. Section 3 describes the quantitative methodology and data sources. Section 4 presents the long-

term trend analysis and the heterogeneous comparative results. Section 5 provides a detailed discussion and interpretation of the complex factors observed, and Section 6 offers the final conclusions and suggestions for future research.

2 Related Work

2.1 Cyber Threat Landscape, Security Governance, and Regulatory Response

The modern healthcare sector is characterized by the increasing network connectivity of medical devices, often referred to as the Internet of Medical Things (IoMT), which has simultaneously exposed critical cybersecurity vulnerabilities [4, 5]. Connected medical devices and the health information they process are attractive targets: the connectivity of IoMT devices exposes them to severe cybersecurity threats that can compromise patient safety and data privacy [1], and the limited resources of many devices constrain the security measures that can be deployed [2]. Beyond data breaches, cyberattacks pose a direct threat to patient safety; for example, the FDA has issued a safety communication on remotely exploitable vulnerabilities in an infusion pump (FRN) [3].

To manage this escalating risk, the focus of governance has shifted from post-market compliance to proactive premarket security assurance. Regulatory bodies, including the FDA, have progressively mandated stronger controls, drawing on established information security governance frameworks such as the NIST Cybersecurity Framework (NIST CSF) [7–10]. The most significant action came through the Consolidated Appropriations Act, 2023, which made it mandatory for medical device manufacturers to submit comprehensive documentation, including Software Bill of Materials (SBOMs) [11], threat modeling reports, and vulnerability management plans, with their 510(k) premarket submissions [5]. This legislative action reflects a global trend toward making software supply chain security a core regulatory requirement [5, 11], necessitating a fundamental, resource-intensive shift in manufacturer design and documentation practices. This global regulatory strengthening includes discussions on national cyber security legislation and governance [12] and the assessment of policy trends in major countries [13]. Selecting security controls in practice also requires weighing risk reduction against implementation cost and mission alignment [14], consistent with the cost-benefit view of security investment [15].

2.2 E-Submission Systems and Regulatory Efficiency

The average 510(k) registration period has varied substantially over time (Section 4.1, Figure 1). To standardize documentation and support complete submissions, the FDA promoted the electronic Submission Template And Resource (eSTAR) and, through final guidance, made its use mandatory for 510(k) submissions from October 1, 2023 [16]. By guiding applicants toward complete submissions, eSTAR was expected to reduce the formal deficiencies that lead to Refuse To Accept (RTA) holds, a potential efficiency gain for the overall clearance timeline [16].

However, the regulatory period analyzed in this study—the mandatory cybersecurity rule enforcement—coincided directly with the mandatory adoption of eSTAR. This simultaneous implementation introduced two contrasting forces impacting the market clearance period: eSTAR promoting efficiency versus the new cybersecurity mandates increasing documentation complexity, thereby imposing a compliance burden of the kind documented for regulatory and security-policy compliance costs in other contexts [15, 17–20]. Studies of regulation in other domains point to heterogeneous effects of compliance requirements on firms and markets [21–23], including for AI/ML-enabled devices [24]. Critically, to the best of the author’s knowledge, the existing literature offers no empirical evidence on whether the efficiency gains from eSTAR would entirely mitigate the initial documentation burden imposed by the new security mandates. The net change in the 510(k) market clearance period depends heavily on the relative strength of these two opposing, largely unquantified, effects.

2.3 Regulation, Innovation, and Heterogeneous Impact in AI/ML Devices

The proliferation of Artificial Intelligence and Machine Learning (AI/ML) enabled medical device software (SaMD) represents one of the most significant challenges to traditional regulatory frameworks [25, 26]. The adaptive nature of AI/ML software presents unique regulatory difficulties due to the inherent unpredictability of its outputs over time [27]. In response, the FDA has established frameworks like the Predetermined Change Control Plan (PCCP) and guiding principles for Good Machine Learning Practice (GMLP), aiming to balance rapid market innovation with robust safety and security [28, 29].

The academic literature suggests that the complexity of demonstrating cybersecurity compliance and robust clinical performance simultaneously creates a potential compliance burden in the clearance process

for innovative products [30, 31]. Furthermore, reviews of the regulation of AI-enabled device software highlight regulatory uncertainty and evolving expectations for novel technologies [32, 33]; to the best of the author’s knowledge, whether this translates into more variable review times has not been quantified. This theoretical background is crucial for interpreting the heterogeneous results expected in this study for innovative product groups, such as the image processing software (QIH) and machine learning notification software (QYE).

2.4 Research Gap and Contribution

In summary, the literature confirms the urgency of strengthening medical device cybersecurity and identifies the theoretical conflict between the efficiency-promoting eSTAR system and the documentation-burdening cybersecurity mandates. However, existing studies have focused predominantly on pre-enforcement predictions, technical requirements, or general policy debates.

Crucially, a quantitative, post-enforcement analysis leveraging long-term market data to assess the net effect of these two contemporaneous regulatory changes on the 510(k) clearance timeline is absent. To the best of the author’s knowledge, this study is the first to empirically analyze the change in the total registration period of the 510(k) market after the October 1, 2023, mandatory rule implementation, quantifying: (1) the overall net effect (efficiency gains vs. compliance burden) and (2) the differential impact across various medical device product categories. A concurrent study by the author examined AI-enabled devices with a difference-in-differences design and a re-extracted dataset [34]; the present study complements it by analyzing the overall market and product-code heterogeneity. By providing this real-world evidence, this research fills a critical gap in the literature on information security governance and regulatory economics in the healthcare sector.

3 Methods

This study utilizes the FDA’s publicly available 510(k) premarket notification database. The analysis dataset comprised 80,749 records with a final decision, covering 2,866 product codes, with decision dates from January 11, 2000, to October 31, 2025. Submissions withdrawn or still under review at the time of data extraction are not part of the extract. This ensures that the dependent variable, Total Registration Period, objectively reflects the duration from the 510(k) submission date to the FDA’s final regulatory outcome.

This study is based on Quantitative Comparative Analysis. Data was divided into the period Pre-

Enforcement ($T=0$) and Post-Enforcement ($T=1$) based on the mandatory cybersecurity regulation, October 1, 2023 (records were assigned to the periods by FDA decision date). The statistical analyses were implemented in Python; the analysis code was written and cross-checked with the assistance of a generative AI tool (Claude, Anthropic; see the Artificial Intelligence Usage Declaration), and the results were verified by the author against the source data.

Table 1. Key analysis variables. The product codes mentioned in the paper, their descriptions and the key regulatory impact findings are explained in S1 of the supporting information; a statistical summary of the product codes is provided in S2.

Variable type	Variable name	Definition
Independent variable	Regulation period (S)	pe- $T = 0$: FDA decision date before October 1, 2023; $T = 1$: decision date on or after October 1, 2023
Dependent variable 1	Average registration period (days) for 510(k) by period (T)	Average review time period (days) for 510(k) by period and product code
Dependent variable 2	Submission volume (N)	Total number of 510(k) submissions by period and product code
Group variable	Product code (C)	Individual medical device product code classified by the FDA (e.g., FRN, LLZ, QIH)

The analysis procedure includes:

1. Long-term Trend Analysis: Visualizing the trend of the average registration period by year from 2000 to the present.
2. Pre- and Post-Regulation Comparative Analysis: Dividing the total registrations into pre- and post-enforcement periods to confirm the overall change in the average registration period. For inferential statistical comparison of the overall average duration, the Welch's T-test was employed, which is suitable for comparing the means of two groups with potentially unequal variances.
3. Data Filtering for Robustness: To ensure the robustness of the inferential statistical analysis against outliers, data outside the 5th and 95th percentiles (5%-95% IQR filtered dataset) were excluded for the overall comparison of average registration periods. Specifically, the 5th and 95th percentile bounds of the Total Registration Period were computed once from the pooled (pre- and post-regulation combined) distribution, and these same bounds were then applied to filter both the pre-regulation and post-regulation groups. This pooled-bound ap-

proach ensures that both groups are filtered against a common, consistent reference distribution rather than group-specific bounds, which could otherwise distort the comparison. A sensitivity analysis was additionally conducted at 1%-99% and 10%-90% thresholds, using the same pooled-bound procedure, to confirm that the direction and approximate magnitude of the finding are not dependent on the specific choice of the 5% cutoff (see Section 5.1).

4. Heterogeneous Impact Analysis: Detailed calculation of the change in the average registration period (ΔT) and the change in submission volume (ΔN) for each Product Code. This analysis concretely derives the differential impact of the regulation on high-risk product groups (FRN, LLZ, etc.) and emerging technology product groups (QIH, etc.). For product codes with at least 10 submissions in each period (152 codes), review times were compared with two-sided Mann-Whitney U tests, and the 152 p-values were adjusted with the Benjamini-Hochberg false-discovery-rate (FDR) procedure (Bonferroni-adjusted results are also reported in the Results). Product codes with fewer than 10 submissions in either period are reported descriptively without inference. Because the post-regulation window (October 2023 to October 2025; about 2.1 years) is much shorter than the pre-regulation window (about 23.7 years), ΔN is accompanied by annualized submission rates (submissions per year); codes with no pre-regulation submissions have an undefined ΔT .

The impact of the new mandatory cybersecurity regulation is quantified by measuring the differential change in two key market indicators for each product code (C) before (T_0 , N_0) and after (T_1 , N_1) the October 1, 2023, enforcement date:

$$\Delta T = T_1 - T_0, \quad \Delta N = N_1 - N_0 \quad (1)$$

Where, T_0 is the average registration duration (in days) before the regulation, T_1 is the average duration after the regulation, N_0 and N_1 represent the submission volume (number of cases) before and after the regulation, respectively. Specifically, ΔT serves as the primary dependent variable, quantifying the net effect of the opposing regulatory factors (efficiency gains vs. compliance burden). A positive value for ΔT indicates that the compliance burden prevailed, while a negative value suggests efficiency gains were dominant. ΔN acts as a secondary indicator, reflecting the regulatory impact on manufacturer market entry activity within that product code.

5. Interpretation of Results: Comprehensively in-

interpreting how the efficiency effect of the eSTAR mandate and the documentation complexity effect of the cybersecurity regulation interacted to produce the observed results across different product codes.

4 Results

4.1 Change in Average Registration Period

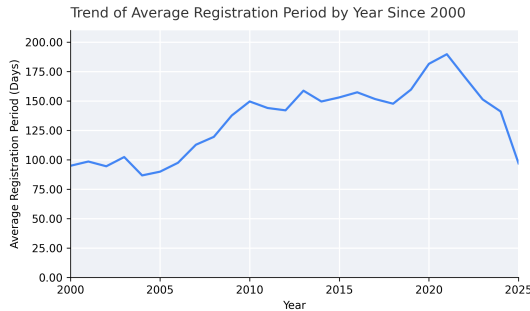


Figure 1. Trend of average registration period by year since 2000

The order of writing in [Figure 1](#) above and the detailed figures for the Average Registration Period by year are explained in S3 and S4 of supporting information.

[Figure 1](#) shows the trend of the average registration period by year since 2000. The FDA 510(k) average registration period from January 1, 2000, to October 31, 2025, has shown long-term variability.

- **Stabilization in the Early 2000s:** The period remained stable, ranging from about 86 to 102 days, from approximately 95 days in 2000 until 2005.
- **Increasing Trend from 2006 to 2013:** The review period showed a tendency to gradually increase, reaching approximately 159 days in 2013.
- **Resurgence in 2019 to 2021:** The average registration period increased again, reaching a peak of approximately 190 days in 2021.
- **Decreasing Trend Since 2022:** The average registration period began to decrease again from 2022. The average period for 2025 is approximately 97 days, but this partial-year value is right-censored (see below) and should not be read as a return to the previous stabilization level. This initial post-2022 decline from the 2021 peak primarily represents the FDA's institutional recovery from the intense COVID-19 review backlog. Crucially, this pandemic recovery dynamic intersects directly with the implementation of the new mandatory cybersecurity regulations and the eSTAR submission mandate. Consequently, this recent downward trend reflects a complex administrative normalization

rather than a simple reduction in regulatory scrutiny. Three overlapping dynamics should be disentangled when interpreting the 2022–2025 trend: (1) backlog recovery, as the FDA worked through the accumulated review queue from the COVID-19 pandemic, which by itself would tend to shorten average review times over this period; (2) eSTAR adoption, which was expected to improve submission completeness and reduce early-stage rejections, also tending to shorten average times; and (3) the cybersecurity documentation burden introduced in October 2023, which tends to lengthen average times. The 2025 figure is based on records received and decided through October 31, 2025; slower 2025 submissions are not yet decided and are therefore absent, so this value understates the eventual review time of 2025 submissions. Taken together, the observed 2022–2025 trajectory likely reflects the net result of two shortening forces (backlog recovery, eSTAR) partially offsetting one lengthening force (cybersecurity documentation), rather than any single mechanism acting in isolation.

4.2 Overall Change in Registration Period Before and After Cybersecurity Regulation

A comparison of the average registration period for all 510(k) registrations before and after the mandatory cybersecurity regulation implementation date of October 1, 2023, is shown in [Table 2](#). As shown in [Table 2](#), the pre-regulation period ($N = 74,015$) is substantially larger than the post-regulation period ($N = 6,734$), reflecting the recent enforcement date and the correspondingly shorter observation window available for post-regulation data; this sample-size imbalance is a limitation discussed further in [Section 5.2](#).

Table 2. Comparison of average registration periods before and after the implementation of cybersecurity regulations. S5 of the supporting information provides additional detail.

Period	Submission volume (cases, N)	Average registration period (days, mean)	Standard error (SE)
Before ($T = 0$)	74,015	131.70	0.42
After ($T = 1$)	6,734	154.75	1.46

Note: Welch's $t = -15.21$, $p < 0.001$, 95% CI of the difference = [20.08, 26.02] days. [Table 2](#) presents a raw comparison of the unfiltered full dataset. The statistically significant findings in [Section 4.2](#) (an increase of 20.92 days, $p < 0.001$) are derived from a 5%–95% IQR-filtered dataset, a methodology utilized to ensure the robustness of the inferential statistical analysis.

The raw comparison of the unfiltered full dataset in [Table 2](#) shows an increase of 23.05 days (from

131.70 to 154.75 days), consistent with the 95% CI of [20.08, 26.02] days reported above. However, this raw comparison does not account for the statistical robustness necessary for inferential conclusions, as it is modestly influenced by a small number of extreme outliers in the very large pre-regulation dataset.

Key Statistical Finding: When conducting the comparative analysis using the 5%-95% IQR filtered dataset (Welch's $t = -19.28$, $p < 0.001$, $SE = 1.09$), the average registration period showed a statistically significant increase of 20.92 days. This filtered estimate is closely consistent with the raw, unfiltered estimate (23.05 days), indicating that the finding is robust to the exclusion of extreme outliers rather than being an artifact of a small number of anomalous cases. This indicates that the post-regulation period was associated with a statistically detectable delay in the overall clearance process, despite the contemporaneous efficiency-promoting factors of eSTAR (see Section 5.2 for the limits of causal interpretation).

Submission Volume: The post-regulation period ($T=1$) comprised 6,734 registrations, which represents a significantly smaller sample size compared to the 74,015 registrations in the pre-regulation period ($T=0$) due to the recent cut-off date.

4.3 Heterogeneous Analysis of Changes in Submission Volume and Period by Product Code

The regulatory impact, quantified by ΔT (change in average period) and ΔN (change in submission volume), varied greatly by product code, indicating heterogeneous impact depending on product characteristics. Of the 2,866 product codes in the dataset, 974 had submissions in both periods, and 152 had at least 10 submissions in each period; these 152 codes were tested individually (Mann–Whitney U test; S6), with false-discovery-rate (FDR) correction across the 152 tests. Product codes with fewer than 10 submissions in either period are described without inference (S5). Because the post-regulation window (October 2023 to October 2025; about 2.1 years) is much shorter than the pre-regulation window (about 23.7 years), ΔN is reported together with annualized submission rates in S5.

A. Heterogeneity Across Tested Product Codes: Among the 152 tested codes, 51 showed a nominally significant difference in review time ($p < 0.05$; about 8 would be expected by chance), and 39 remained significant after FDR correction (15 after Bonferroni correction). Of the 51 nominally significant codes, 37 showed longer and 14 shorter review times after the regulation. Across all 152 codes, the median ΔT was +10.5 days, and ΔT was positive in 59.2% of

codes. Delays were therefore concentrated in a subset of codes rather than uniform across the market.

B. Product Codes Discussed in This Paper (ΔT ; see S5 for all values): The change in the average registration period varied across the product codes discussed in this paper, highlighting the differential impact of the combined regulatory factors.

- **Picture Archiving and Communication Systems (LLZ):** The clearest, statistically robust delay among the codes discussed here. The mean review time rose from 99.5 to 165.1 days ($\Delta T = +65.6$ days; median 71.0 to 163.5 days; $N = 1,854$ to 130; $p < 0.001$, $FDR\ q < 0.001$).
- **Infusion Pumps (FRN):** The mean review time rose from 126.4 to 211.4 days ($\Delta T = +85.0$ days; median 81.5 to 130.0 days; $N = 198$ to 15), but the difference was not statistically significant ($p = 0.070$; $FDR\ q = 0.18$), reflecting the small post-regulation sample.
- **AI-Based Image Processing Software (QIH):** The mean review time fell from 171.9 to 150.5 days ($\Delta T = -21.4$ days; $N = 83$ to 164), with nearly identical medians (142.0 vs. 141.5 days). The change was not statistically significant ($p = 0.43$; $FDR\ q = 0.68$).
- **Orthodontic Software (PNN):** The mean review time fell from 182.8 to 122.3 days ($\Delta T = -60.5$ days; $N = 23$ to 7). The unadjusted Mann–Whitney p was 0.044, but only 7 post-regulation submissions were available (fewer than 10), so this result is exploratory and was not tested within the FDR-corrected set.
- **Codes With Too Few Submissions for Testing:** QYE (machine learning-based notification software for reduced ejection fraction; $N = 1$ to 4; 23.0 to 174.8 days), QMI (1 to 1; 27 to 266 days), OMT (1 to 1; 1,342 to 126 days), and PBP (1 to 1; 109 to 265 days) each have a single pre-regulation observation, so their ΔT values are anecdotal and cannot be tested. SBF, SCA, QYA, QXQ, and SAN have no pre-regulation submissions in the dataset, so ΔT is undefined for them.

C. Submission Volume (ΔN ; annualized rates in S5): Among the codes discussed here, QIH showed the largest growth, from 83 to 164 submissions (3.5 to 78.6 per year, about 22-fold), and NGL rose from 5 to 17 (0.2 to 8.1 per year). SBF (0 to 17; 8.1 per year) and SCA (0 to 8; 3.8 per year) first appear in the post-regulation period. In contrast, LLZ declined from 1,854 to 130 submissions (78.1 to 62.3 per year, -20%) and FRN from 198 to 15 (8.3 to 7.2 per year, -14%). PNN fell in raw count (23 to 7) but rose in annualized terms (1.0 to 3.4 per year).

Taken together, the code-level results show that, although the overall clearance process took longer after the regulation, the change was uneven: delays were concentrated in a subset of codes (notably image-management software such as LLZ), whereas other codes showed no significant change or shorter review times. Because most product codes contributed few post-regulation submissions, code-level results outside the 152 tested codes are exploratory.

5 Discussion

5.1 Interpretation of Complex Factors for Change in Average Registration Period

The research found that the overall 510(k) average registration period statistically significantly increased by 20.92 days ($t = -19.28$, $p < 0.001$, $SE = 1.09$) after the mandatory cybersecurity regulation was implemented. This result is contrary to the expectation that eSTAR's efficiency gains would largely offset the added cybersecurity documentation burden. This result is consistent with the hypothesis that the burden of creating new cybersecurity documentation (compliance burden) statistically outweighed the efficiency effect of the mandatory eSTAR (efficiency gains). However, as discussed in Section 5.2, this observational study design cannot fully separate the cybersecurity-documentation effect from other contemporaneous confounders, including eSTAR's own adoption learning curve and post-pandemic review dynamics.

This finding is notable because the mandatory eSTAR template was introduced to streamline submissions [16], yet the overall registration period was longer after the regulation. Instead, the observed statistically significant difference suggests a substantial regulatory burden, although part of it may reflect the confounders and the comparison-period sensitivity discussed in Section 5.2. From an information security governance perspective, the 20.92-day difference is consistent with the time manufacturers need to integrate security into their design and documentation practices, emphasizing that compliance demands a shift towards 'Security by Design' rather than a simple 'end-of-pipeline' document checklist.

The heterogeneous impact remains crucial: while the overall trend showed a delay, review times changed unevenly across product codes (Section 4.3). Delays were concentrated in a subset of codes, most clearly in picture archiving and communication systems (LLZ; +65.6 days, FDR $q < 0.001$), a software-centered category that handles large volumes of patient images and related health information. In contrast, AI-based image processing software (QIH) showed no statistically significant change (-21.4 days; $p = 0.43$), and the machine learning-based notification software code

QYE had only a single pre-regulation observation, so no inference is possible. AI/ML-enabled devices pose distinctive regulatory challenges [24], which may add variability to review cycles during the initial phase of new guidelines; the present data neither confirm nor refute such an effect for QIH. This underscores the usefulness for AI/ML developers of proactively adopting frameworks such as PCCP to minimize submission unpredictability. Single-observation changes in codes such as OMT should not be interpreted; they could reflect factors outside the scope of the cybersecurity rule, such as strategic shifts in manufacturer submission practices (e.g., expanded use of Q-Submission).

The observed discrepancy between the raw mean and the filtered mean highlights the inherent volatility of FDA 510(k) clearance timelines. The raw increase of 23.05 days is modestly affected by a small number of extreme outliers in the vast pre-regulation dataset ($N = 74,015$). When these outliers—which do not represent the typical manufacturer experience—are removed through 5%–95% IQR filtering, a closely consistent, statistically significant delay of 20.92 days emerges ($p < 0.001$). This is consistent with the interpretation that for the core 90% of the market, the increased documentation burden of the 2023 cybersecurity mandate may have prolonged the clearance process.

5.2 Addressing Confounding Factors and Limitations

While the data show a clear difference after the regulation, several contemporaneous confounding factors must be acknowledged.

- **Transitional Learning Curve:** The mandatory adoption of eSTAR may have introduced a temporary “learning curve” for both manufacturers and FDA reviewers, which could act as a transitional delay factor independent of cybersecurity requirements. Because the cybersecurity mandate and the eSTAR requirement became effective on the same date, this observational, before-after study design cannot fully separate the two effects statistically; the 20.92-day estimate should therefore be interpreted as the combined effect of both contemporaneous regulatory changes, not as an isolated measure of the cybersecurity-documentation burden alone.
- **Post-Pandemic Dynamics:** The study period coincides with the FDA's recovery from COVID-era review backlogs, which may influence long-term trend comparisons.
- **Sample Size Constraints:** Due to the recent enforcement date, the post-regulation sample ($N = 6,734$) is significantly smaller than the pre-

regulation baseline ($N = 74,015$). Consequently, code-level changes in product codes with fewer than 10 submissions in either period (e.g., QYE, OMT, QYA) are reported descriptively and should be interpreted as anecdotal observations rather than core results.

- **Incomplete 2025 Data:** The dataset includes records received and decided through October 31, 2025 (Data Availability Statement). Because submissions received in 2025 appear only if they had already been decided by that date, slower submissions are missing, and the 2025 value in Fig. 1 (96.96 days, by year of receipt) is right-censored; it should not be read as a return to earlier review times. The pre- and post-regulation comparison in Table 2 groups records by decision date and is therefore not truncated in the same way; however, the post-regulation window covers only about 25 months, which limits precision and generalizability.
- **Cohort Definition and Baseline:** Periods were assigned by FDA decision date. Consequently, 23.9% of post-regulation decisions (1,608 of 6,734) concerned submissions received before October 1, 2023, which were not subject to the new requirements and had a longer mean review time (235.4 days) than later submissions (129.4 days). In a sensitivity analysis defining periods by submission date and restricting both groups to reviews completed within 300 days (S7), the post-regulation mean exceeded that of all earlier submissions by 24.9 days ($p < 0.001$) but that of submissions received in January 2021 to September 2023 by only 1.3 days ($p = 0.55$). The overall difference therefore partly reflects the long-run rise in review times since the early 2000s and cannot be attributed in full to the regulation.
- **Relation to a Concurrent Analysis:** A concurrent study by the author [34], using a re-extracted FDA dataset (83,675 records through August 2026, De Novo excluded) and a difference-in-differences design with product-code-clustered standard errors, found no significant post-rule change for the overall market after adjustment for submission type and review pathway, and found the increase concentrated in radiology-panel imaging and treatment-planning codes, including LLZ, while the highest-volume AI code (QIH) showed no significant change after correction. These findings are consistent with the code-level concentration of delays and with the comparison-period sensitivity reported here, and they indicate that the overall before-after difference reported in this paper should be interpreted with caution rather than as a market-

wide effect of the regulation.

5.3 Regulatory Impact and Implications for Security Governance

The product groups analysed as high-risk in this study present direct implications for risk management and security frameworks.

- **High-Risk Patient Safety Devices (FRN):** Infusion pumps (FRN), which are directly related to patient safety, showed a numerically large increase in mean review time (+85.0 days, from 126.4 to 211.4 days; median 81.5 to 130.0 days) after the regulation ($N = 198$ pre-regulation, $N = 15$ post-regulation), but the difference was not statistically significant ($p = 0.070$). Given the small post-regulation sample, the direction is consistent with heightened review intensity for patient-safety devices, though this cannot be confirmed. Irrespective of review time, the patient-safety criticality of infusion pumps calls for rigorous application of ISO 14971 (Risk Management) principles, with manufacturers formally documenting how new cybersecurity requirements mitigate severe patient harm scenarios.
- **Data Integrity and PHI-Handling Software (LLZ):** Picture archiving and communication systems (LLZ) manage large volumes of patient images and related health information and are therefore potentially susceptible to refuse-to-accept (RTA) actions or additional information requests if documentation on data integrity and Denial-of-Service (DoS) defense is incomplete. The mean review time for LLZ rose by 65.6 days (99.5 to 165.1 days; $p < 0.001$, FDR $q < 0.001$), the clearest code-level delay in this study, although this observational result cannot establish that documentation requirements were the cause. At the same time, annualized LLZ submissions declined by about 20% (78.1 to 62.3 per year), so possible unintended effects on market entry in high-volume software categories warrant further assessment by regulators.
- **Innovation and Compliance Balance (QIH/AI Software):** AI-based image processing software (QIH) showed rapid growth in submissions (83 to 164; 3.5 to 78.6 per year) but no statistically significant change in review time (−21.4 days; $p = 0.43$), while the single pre-regulation observation for QYE precludes inference. The results therefore do not show that novel AI-enabled devices experienced longer reviews. A reasonable implication, which these data cannot test directly, is that early and complete adoption of cybersecurity standards, as mandated by the

FDA, is the main control against unpredictable review timelines for novel devices; larger post-enforcement datasets are required to establish definitive security governance benchmarks for emerging technologies.

6 Conclusion

This study conducted a quantitative, post-enforcement analysis using large-scale FDA market data to examine the association between the new mandatory cybersecurity regulations and the 510(k) clearance timeline, moving the academic discourse beyond theoretical prediction toward empirical evidence.

The core finding is that, after the FDA cybersecurity regulation took effect, the overall average registration period was 20.92 days longer ($p < 0.001$; 5%-95% IQR-filtered estimate, closely consistent with a raw estimate of 23.05 days). This difference is consistent with an increased burden of cybersecurity documentation outweighing the efficiency gains of the mandatory eSTAR system, but it cannot be attributed to the regulation alone: the design cannot separate the cybersecurity effect from eSTAR's own adoption learning curve and post-pandemic review dynamics, and the difference fell to about 1 day when the post-regulation period was compared with submissions received in 2021 to 2023 rather than with the full 2000 to 2023 history.

These findings suggest implications for information security governance: the review burden may have shifted from 'formal completeness (eSTAR)' toward the 'substantive security quality (cybersecurity)' of the documentation. The observed association with longer reviews, clearest in picture archiving and communication systems (LLZ), is consistent with the view that information security assurance requires a time-intensive shift toward Security by Design within the medical device lifecycle, although it does not by itself quantify the resource commitment required for regulatory compliance. Furthermore, the heterogeneous results observed across product codes underscore the need for flexible, risk-based regulatory enforcement, particularly in rapidly evolving areas like AI/ML.

Future research should focus on two critical areas: First, analyzing the frequency and specific reasons for the FDA's Additional Information Requests (AI Request) is essential for identifying which cybersecurity elements reviewers strictly examine, providing a clear focus for industry security controls. Second, there is a clear necessity to quantitatively study the impact of regulatory compliance costs on the market entry of Small and Medium Enterprises (SMEs) to assess the long-term barrier-to-entry effect of the new security mandates on innovation and competition [35].

Data Availability Statement

All relevant data are within the paper and its Supporting information files. Data for 2025 are incomplete: records are included only if received and decided by October 31, 2025, so the 2025 average (96.96 days, by year of receipt) is right-censored because slower 2025 submissions have not yet been decided.

Acknowledgment

The author received no specific funding for this work. The author would like to express their profound gratitude to the HUINNO Co., Ltd. RAQA Team for providing the crucial FDA 510(k) registration data and regulatory insights that formed the empirical foundation of this study. This research would not have been possible without their essential support and expertise in navigating the complex landscape of medical device regulation.

Artificial Intelligence Usage Declaration

During the preparation and revision of this work, the author used Claude (Anthropic; Claude Sonnet 5.5, accessed through the claude.ai interface) for the following purposes: (i) drafting and editing text, including revisions made in response to peer review (softening causal language, adding limitations, and restructuring sections); (ii) writing and running Python code to re-run and cross-check the statistical analyses on the public FDA 510(k) dataset, including the product-code analysis and the sensitivity analyses reported in this paper; (iii) checking bibliographic details of references against online sources; (iv) redrawing Figure 1 from the data in Supporting Information S4 with Python plotting code (no generative image model was used); and (v) converting the manuscript and supporting tables to the journal's LaTeX template. This use went beyond language editing. The AI-assisted checks identified several errors in earlier versions of the manuscript, including a non-existent product code, test statistics that were inconsistent with the reported estimates, and inaccurate bibliographic entries; these were corrected in this version. After using this tool, the author reviewed and edited the content as needed, verified the reported statistics against the source data, and takes full responsibility for the content of the publication. No AI tool is listed as an author.

References

- [1] S. Deb, E. Lupu, E. M. Drakakis, A. A. Bharath, Z. K. Leung, G. R. Ma, and A. Chattopadhyay. Securing the internet of medical things (IoMT): real-world attack taxonomy and prac-

- tical security measures, 2025. arXiv preprint arXiv:2507.19609.
- [2] A. Waqas. Performance evaluation of deep learning models on diverse IoT datasets for intrusion detection. *The ISC International Journal of Information Security*, 18(1):19–33, 2026. .
 - [3] U.S. Food and Drug Administration. Cybersecurity vulnerabilities of Hospira Symbiq infusion system: FDA safety communication, 2015. Jul 31. Available from: <http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm>.
 - [4] U.S. Congress. Federal food, drug, and cosmetic act (FD&C act), section 524b – ensuring cybersecurity of medical devices, 2023. [Internet]. Available from: <https://www.congress.gov/bill/117th-congress/house-bill/2617/text>.
 - [5] U.S. Food and Drug Administration. Cybersecurity in medical devices: Quality system considerations and content of premarket submissions, 2023. [Internet]. Available from: <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions>.
 - [6] AAMI News. FDA explains medical device cybersecurity requirements, 2024. [Internet]. 2024 Feb 22. Available from: <https://array.aami.org/content/news/aami-fda-nexus-medical-device-cybersecurity-requirements-jessica-wilkerson>.
 - [7] G. B. White and N. Sjin. The NIST cybersecurity framework. In *Research Anthology on Business Aspects of Cybersecurity*. IGI Global, 2022.
 - [8] A. Amiruddin, H. G. Afiansyah, and H. A. Nugroho. Cyber-risk management planning using NIST CSF v1.1, NIST SP 800-53 rev. 5, and CIS controls v8. In *Proceedings of the 3rd International Conference on Informatics, Multimedia, Cyber, and Information System (ICIMCIS)*, pages 19–24. IEEE, 2021.
 - [9] E. H. N. Safitri and H. Kabetta. Cyber-risk management planning using NIST CSF v1.1, ISO/IEC 27005:2018, and NIST SP 800-53 revision 5 (a study case to ABC organization). In *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*, pages 332–338. IEEE, 2023.
 - [10] D. Sulistyowati, F. Handayani, and Y. Suryanto. Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *JOIV: International Journal on Informatics Visualization*, 4(4):225–230, 2020. .
 - [11] B. Xia, T. Bi, Z. Xing, Q. Lu, and L. Zhu. An empirical study on software bill of materials: Where we stand and the road ahead. In *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*, pages 2630–2642, 2023. arXiv:2301.05362.
 - [12] M. Ostermann, R. Mathias, F. Jahed, M. B. Parker, F. D. Hudson, W. C. Harding, S. Gilbert, and O. Freyer. Cybersecurity requirements for medical devices in the EU and US – a comparison and gap analysis of the MDCG 2019-16 and FDA premarket cybersecurity guidance. *Computational and Structural Biotechnology Journal*, 28:259–266, 2025. .
 - [13] S. Zhang, Y. Li, W. Liu, Q. Chu, S. Wang, J. Li, and Y. Chen. A decade of review in global regulation and research of artificial intelligence medical devices (2015–2025). *Frontiers in Medicine*, 12:1630408, 2025. .
 - [14] S. Yousefi Mashhour, M. Dehghan, B. Sadeghian, and A. Hashemi Golpayegani. Mission-centric countermeasure selection in cybersecurity situation awareness systems. *The ISC International Journal of Information Security*, 2026. . In press.
 - [15] L. A. Gordon, M. P. Loeb, and L. Zhou. Integrating cost–benefit analysis into the NIST cybersecurity framework via the Gordon–Loeb model. *Journal of Cybersecurity*, 6(1):tyaa005, 2020. .
 - [16] U.S. Food and Drug Administration. Electronic submission template for medical device 510(k) submissions; guidance for industry and food and drug administration staff; availability, 2022. Federal Register, Sep 22. Available from: <https://govinfo.gov/content/pkg/FR-2022-09-22/pdf/2022-20572.pdf>.
 - [17] W. Wu and S. Liu. Compliance costs of AI technology commercialization: A field deployment perspective, 2023. arXiv preprint arXiv:2301.13454.
 - [18] S. Eichfelder and F. Hechtner. Tax compliance costs: Cost burden and cost reliability. *Public Finance Review*, 46(4):618–644, 2018.
 - [19] J. Slemrod. Tax compliance and enforcement. *Journal of Economic Literature*, 57(4):904–954, 2019. .
 - [20] J. D’Arcy and P. B. Lowry. Cognitive-affective drivers of employees’ daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29(1):43–69, 2019.
 - [21] Y. Wang, X. Sun, and X. Guo. Environmental regulation and green productivity growth: Empirical evidence on the Porter hypothesis from OECD industrial sectors. *Energy Policy*, 132: 611–619, 2019.
 - [22] K. E. Maskus and J. S. Wilson, editors. *Quantifying the Impact of Technical Barriers to Trade*:

- Can It Be Done?* University of Michigan Press, Ann Arbor, 2001.
- [23] J. E. Maule. COUNTERPOINT: Although theoretically appealing, simplified filing systems entail too many risks of security, resource, and compliance costs. *ABA Tax Times*, 36(1), 2016.
- [24] S. Gerke, B. Babic, T. Evgeniou, and I. G. Cohen. The need for a system view to regulate artificial intelligence/machine learning-based software as medical device. *npj Digital Medicine*, 3(1):53, 2020. .
- [25] G. Joshi, A. Jain, S. R. Araveeti, S. Adhikari, and H. Garg. FDA-approved artificial intelligence and machine learning (AI/ML)-enabled medical devices: an updated landscape. *Electronics*, 13(1):145, 2024.
- [26] S. Reddy. Global harmonization of artificial intelligence-enabled software as a medical device regulation: addressing challenges and unifying standards. *Mayo Clinic Proceedings: Digital Health*, 2025.
- [27] A. Shrivastava, U. Jain, M. Al-Farouni, Y. Kumar, R. J. Anandhi, and M. Bhavana. Proposed framework for modifications to artificial intelligence/machine learning (AI/ML)-based software as a medical device (SaMD). In *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)*, pages 1755–1763. IEEE, 2024. .
- [28] S. G. Odaibo. Risk management of AI/ML software as a medical device (SaMD): on ISO 14971 and related standards and guidances, 2021. arXiv preprint arXiv:2109.07905.
- [29] V. Singh, S. Cheng, A. C. Kwan, and J. Ebinger. United states Food and Drug Administration regulation of clinical software in the era of artificial intelligence and machine learning. *Mayo Clinic Proceedings: Digital Health*, 2025.
- [30] A. G. Fraser, E. Biasin, B. Bijmens, N. Bruining, E. G. Caiani, K. Cobbaert, R. H. Davies, S. H. Gilbert, L. Hovestadt, E. Kamenjasevic, Z. Kwade, G. McGauran, G. O'Connor, B. Vasey, and F. E. Rademakers. Artificial intelligence in medical device software and high-risk medical devices – a review of definitions, expert recommendations and regulatory initiatives. *Expert Review of Medical Devices*, 20(6):467–491, 2023. .
- [31] K. A. Cepeda Zapata, T. Ward, R. Loughran, and F. McCaffery. Challenges associated with the adoption of artificial intelligence in medical device software. In L. Longo and R. O'Reilly, editors, *Artificial Intelligence and Cognitive Science (AICS 2022)*, volume 1662 of *Communications in Computer and Information Science*, pages 163–174. Springer, Cham, 2023. .
- [32] Y. Han, A. Ceross, and J. Bergmann. Regulatory frameworks for AI-enabled medical device software in China: comparative analysis and review of implications for global manufacturer. *JMIR AI*, 2024.
- [33] S. A. Ebad, A. Alhashmi, M. Amara, A. B. Miled, and A. R. Ali. Artificial intelligence-based software as a medical device (AI-SaMD): a systematic review. *Healthcare*, 13(3):367, 2025.
- [34] C. Lee. Networked radiology imaging and treatment planning systems and FDA cybersecurity regulation: a difference-in-differences analysis of 510(k) clearance delays. *Journal of Imaging Informatics in Medicine*, 2026. . Online ahead of print.
- [35] J. Maci and P. Marešová. Critical factors and economic methods for regulatory impact assessment in the medical device industry. *Risk Management and Healthcare Policy*, 15:71–91, 2022. .



Chuelwon Lee received the Ph.D. degree in Medical Device Industrial Engineering from Dongguk University, Seoul, Republic of Korea, in 2023. He is a Regulatory Affairs (RA) Specialist at HUINNO Co., Ltd., Seoul, where he works on U.S. FDA 510(k) and EU MDR regulatory activities. His work spans medical device regulatory compliance, embedded signal processing, and quality management, and he has published in biomedical engineering and public health.