Reducing Biomedical Device Risk Without Disrupting Clinical Workflow Is Feasible

Authentication- and monitoring-focused controls aligned to NIST CSF 2.0

Abdalla Ismail · CYBR-698 · Dec 2025 · github.com/Abdi6191/capstone-reproducibility

Biomedical devices remain a high-risk blind spot

- Vendor-controlled patching leaves devices exposed for extended periods
  - Shared credentials and weak authentication persist in clinical environments
  - Patient safety risk rises when security controls are avoided to protect workflow

Prior research supports compensating controls over patching

- FDA (2025): Patching delays are systemic for connected medical devices
  - HSCC (2024): Compensating controls required when OEM timelines dominate
  - Cobrado et al. (2024): Context-aware authentication improves usability

Risk is evaluated through reproducible execution artifacts

- Flow: Synthetic device logs → Reproducible script → Metric output → Control alignment
  - Measures: Account-Monitored Execution Rate
  - Measures: Artifact presence and authentication enforcement consistency

Design is anchored to CSF and Zero Trust principles

- CSF PR.PS-02 (Appendix A, p.24): “Software is maintained, replaced, and removed commensurate with risk.”
  - How satisfied: Compensating authentication and monitoring controls mitigate delayed patching risk
  - Zero Trust Tenet (SP 800-207, p.14): “All data sources and computing services are considered resources.”
  - How satisfied: Biomedical devices are treated as managed, monitored resources

Operational safeguards limit harm and misuse

- Ethics: Fully synthetic logs; no PHI, no real device identifiers
  - Data handling: Encrypted storage, limited retention, version-controlled repo
  - Supplier risk: Vendor patch dependency mitigated via monitoring controls

Risk reduction is measurable and traceable

- SMART metrics: Account-Monitored Execution Rate; Artifact Presence Rate; Auth Enforcement Coverage
  - Traceability: Risk → 800-171r3 03.01.01 → Metric → docs/metric.txt

This work moves CSF outcomes from ad-hoc to defined

- Outcome: PR.PS-02
  - Current: Inconsistent patching; limited monitoring of biomedical device execution
  - Target: Defined compensating controls with reproducible, auditable evidence
  - CSF text (Appendix A, p.24): “Software is maintained, replaced, and removed commensurate with risk.”