Initial post: Medical Implants

Secure design, vulnerability management, and ethical responsibility in medical technologies become particularly salient when a cybersecurity flaw is identified but dismissed as negligible compared to the medical risks of intervention. This is the case with Corazon, a company that developed a Bluetooth-enabled cardiac implant connected to a mobile application. The vulnerability based on a hardcoded value allowing unauthorised remote reboot was acknowledged but left uncorrected. The medical rationale, invoking the invasiveness of surgical replacement, justified inaction despite direct consequences for patient monitoring: device reset, loss of clinical data, and disruption of continuity. This rationale is directly challenged by Freyer et al. (2024), who argue that minimising a technical vulnerability on the grounds of medical risk violates the principles of responsible risk-benefit assessment in healthcare. The argument of close physical proximity is also misleading, as medical environments offer ideal conditions for discreet exploitation. More critically, the absence of compensatory safeguards such as a security proxy, application-level filtering, or active system logging combined with a lack of transparency about system limitations, raises clear ethical concerns regarding Corazon's risk governance.

An analysis through the ACM Code of Ethics (2018) highlights several clear breaches. While principles 1.1 (human wellbeing) and 2.6 (professional competence) may appear respected through the use of open standards and openness to researcher scrutiny principle 1.2 (avoid harm) is undermined by the presence of a hardcoded credential in a non-updatable device. This is formally classified as a critical vulnerability under CWE-798 (MITRE, 2024) and listed among the highest-risk issues in embedded systems by OWASP (2021). Furthermore, both FDA guidance (2023) and NIST SP 800-53 Rev. 5 (2020) emphasise the need for devices to be correctable or mitigated in case of cybersecurity flaws. Corazon's refusal to consider alternatives software patches, hardware proxies, or layered monitoring directly contravenes principles 2.9 (system protection), 2.5 (risk evaluation), and 3.7 (heightened responsibility in critical infrastructure). As Williams and Woodward (2015) underline, the failure to actively manage devices post-market constitutes a severe lapse in ethical governance. Additionally, withholding this information from patients violates principle 1.3 (honesty), denying them the possibility of informed consent.

The BCS Code of Conduct offers a complementary ethical framework through its four core duties, all of which are at stake in this case. The duty to the public interest is weakened by the presence of a flaw that compromises continuity of care and by a lack of transparency towards patients. The duty of professional competence is also breached: as Pycroft and Aziz (2018) argue, when a system cannot be modified post-implantation, this limitation should trigger greater rigour at the design stage, or the deployment of effective compensatory controls. The duty to relevant authorities appears superficially fulfilled through regulatory certification, but this is undermined by the failure to formally disclose the flaw and present a mitigation strategy. Finally, the company's engagement with the professional community, though reflected in its bug bounty initiative, loses credibility when identified vulnerabilities are neither addressed nor followed up. This gap between declared intent and applied ethics calls the company's integrity into question.

An ethical approach demands anticipation, mitigation, and correction, even when solutions are partial. Instead, Corazon has normalised a structural vulnerability in a critical system, which is fundamentally incompatible with any responsible design practice. As Das et al. (2021) argue, the obligation to secure medical software should be treated as no less critical than post-operative clinical monitoring. This case illustrates the ethical fragility of connected healthcare systems when security and transparency are deprioritised. While the innovation may address a legitimate clinical need, it loses its ethical standing if it relies on an unpatchable flaw. The violations of both the ACM and BCS codes demonstrate that in the context of connected medicine, cybersecurity, vigilance, and accountability must be integrated from the earliest stages of development.

References :

- ACM, 2018. ACM Code of Ethics and Professional Conduct: Case Studies. Available at: https://www.acm.org/code-of-ethics/case-studies [Accessed 2 May 2025].

- BCS, 2023. BCS Code of Conduct. BCS, The Chartered Institute for IT. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct [Accessed 2 May 2025].

- Das, Nundy, Tschirhart and Goldschlager, 2021. Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices. Heart Rhythm Journal. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC7550052/ [Accessed 4 May 2025].

- FDA, 2023. Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Guidance for Industry and Food and Drug Administration Staff. Available at: https://www.fda.gov/media/119933/download [Accessed 3 May 2025].

- Freyer, Schürmann, Böttinger and Sedlmayr, 2024. Consideration of Cybersecurity Risks in the Benefit-Risk Analysis of Medical Devices: Scoping Review. Journal of Medical Internet Research. Available at: https://www.jmir.org/2024/1/e65528/ [Accessed 5 May 2025].

- MITRE, 2024. CWE-798: Use of Hard-coded Credentials. Available at: https://cwe.mitre.org/data/definitions/798.html [Accessed 3 May 2025].

- NIST, 2020. Security and Privacy Controls for Information Systems and Organizations NIST Special Publication 800-53 Rev. 5. Available at: https://doi.org/10.6028/NIST.SP.800-53r5 [Accessed 3 May 2025].

- OWASP, 2021. OWASP Internet of Things Top 10. OWASP Foundation. Available at: https://owasp.org/www-project-internet-of-things/ [Accessed 3 May 2025].

- Pycroft, L. and Aziz, T.Z, 2018. Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. Expert Review of Medical Devices. Available at: https://www.tandfonline.com/doi/pdf/10.1080/17434440.2018.1483235 [Accessed 4 May 2025].

- Williams, P.A.H. and Woodward, A.J, 2015. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices: Evidence and Research. Available at: https://www.tandfonline.com/doi/full/10.2147/MDER.S50048 [Accessed 4 May 2025].