Peer Response

by Fahad Abdallah - Friday, 16 May 2025, 6:42 PM

Ali, you did a great job providing a positive and wise case study of Corazón. Your effort successfully identifies how ethical computing should not only be excellence in technology but can also respond to patient safety and social responsibility. I especially like your reference to Corazón's involvement with charities that offer free or low-cost implants to low-income individuals. This move shows how a business can combine technological innovation with social impact, which is something other tech companies should consider (Regalado, 2024).

The structure of your interpretation of the ACM Code of Ethics is perfect, illustrated by proper examples. Corazón's action conforms to ACM's principles of taking a positive approach to society, doing no harm, and not violating privacy (Birkett et al., 2023). You also clearly highlight their adherence to regulatory standards, such as the GDPR, which supports their legal and ethical position. Baltazar-Sabbah (2025) further supports your argument, explaining that the availability of advanced medical technologies to underprivileged groups promotes trust in digital health solutions. This is particularly important, as trust remains a significant factor in patient acceptance of connected healthcare technologies.

Your mention of the BCS Code of Conduct was also valuable to me. You rightfully explain how Corazón complies with the standards set by the BCS regarding the prioritization of public benefit, professional competence, and data protection (Lescrauwaet et al., 2022). Further, Voegtlin et al. (2022) reinforce this notion by demonstrating how medical technology can harmonize technical performance with safety and ethical responsibility. Patient risks are minimized through the use of proactive design and rigorous testing in their research.

On the whole, your post presents a balanced and optimistic view of the role that ethical computing can play in both business success and social benefit. It serves as a good reminder that any responsible innovation is not just about meeting technical specifications, but also about living up to moral ideals and the general public good. Well done.

References

Baltazar-Sabbah, B. (2025). *Leading With Corazón: A Latina's Journey Toward Equity and Cultural Humility*. In *Strengthening Equitable Education Through Latina Leaders' Perspectives* (pp. 87-110). IGI Global Scientific Publishing. Available at: https://doi.org/10.4018/979-8-3693-7061-2.ch005 (Accessed:16 May 2025).

Birkett, M., Zia, A. W., Devarajan, D. K., Panayiotidis, M. I., Joyce, T. J., Tambuwala, M. M., & Serrano-Aroca, Á. (2023). Multi-functional bioactive silver- and copper-doped diamond-like carbon coatings for medical implants. Acta Biomaterialia, 167, 54-68. Available at: https://doi.org/10.1016/j.actbio.2023.06.037 (Accessed:16 May 2025).

Lescrauwaet, L., Wagner, H., Yoon, C., & Shukla, S. (2022). *Adaptive legal frameworks and economic dynamics in emerging technologies: Navigating the intersection for responsible innovation*. *Law and Economics*, 16(3), 202-220. Available at: https://doi.org/10.35335/laweco.v16i3.61 (Accessed:16 May 2025).

Regalado, Y. M. (2024). *Pedagogy Del Corazón: Investigating Cultural and Community Practices Embedded in IRW Courses Using the Methodology of Counterstory* (Doctoral dissertation, Texas State University-San Marcos). Available at: https://www.proquest.com/openview/207703507b42924878f366edc534d94e/1?cbl=18750&diss=y&pq-origsite=gscholar (Accessed: 16 May 2025).

Voegtlin, C., Scherer, A. G., Stahl, G. K., & Hawn, O. (2022). Grand Societal Challenges and Responsible Innovation. *Journal of Management Studies*, *59*(1), 1-28. Available at: https://doi.org/10.1111/joms.12785 (Accessed:16 May 2025).

Peer Response

by Fahad Abdallah - Friday, 16 May 2025, 6:56 PM

Stephanie, your analysis of Corazon's Bluetooth-enabled cardiac implant is precise and effective in structuring the ethical issues at the intersection of medical safety and cybersecurity. I was most convinced by your discussion concerning the hardcoded credential vulnerability, as it is a significant weakness that could be exploited and, as such, poses serious problems for patient safety, privacy, and data integrity (George & George, 2023).

Your argumentation on the use of the ACM Code of Ethics is good. In particular, you effectively address the issue of not offering patching, mitigation, or compensatory controls for the vulnerability (Archer, 2024). Principle 1.2, which states the responsibility to avoid harm, is violated when Corazon does not offer controls for the vulnerability. According to George et al. (2021), post-market cybersecurity management is not merely an option, but an essential facet that should be practiced for the safety of patients, especially after the identification of flaws in the market. In strengthening your case, you consistently refer to the guidance from the FDA (2023), which highlights the significance of continuous risk management throughout the lifecycle of medical devices and updates after market release.

Your emphasis on transparency is well-taken. Failure to share information about these risks deprives patients of making informed choices, violating ACM Principle 1.3 and the BCS Code of Conduct in terms of upholding the public interest (Tettey et al., 2024). Thomasian and Adashi (2021) also suggest layered protection and partial mitigations as a responsible step forward, which backs your call for protective measures, even if a complete solution is not immediately at hand.

Overall, your post demonstrates that medical device producers must prioritize making devices cybersecure and transparent throughout their entire production process. Your analysis provides fascinating insights into the use of responsible design, constant monitoring, and forthright communication in maintaining patient safety in connected healthcare settings.

References

Archer, A. P. (2024). *A machine learning approach to associations of data breach characteristics in the healthcare industry* (Doctoral dissertation, National University). Available at: https://www.proquest.com/openview/687632c8890c535630fa0553181f0e38/1?cbl=18750&diss=y&pq-origsite=gscholar (Accessed:16 May 2025).

George, A. S., & George, A. H. (2023). The emergence of cybersecurity medicine: Protecting implanted devices from cyber threats. *Partners Universal Innovative Research*

Publication, 1(2), 93-111. Available at: https://doi.org/10.5281/zenodo.10206563 (Accessed:16 May 2025).

George, S., Silva, L., Llamas, M., Ramos, I., Joe, J., Mendez, J., Salazar, R., Tehan, J., Vasquez, T., Nealy, S., & Balcazar, H. (2021). The development of a novel, standards-based core curriculum for community-facing, clinic-based community health workers. *Frontiers in Public Health*, 9, 663492. Available at: https://doi.org/10.3389/fpubh.2021.663492 (Accessed:16 May 2025).

Tettey, F., Parupelli, S. K., & Desai, S. (2024). A review of biomedical devices: Classification, regulatory guidelines, human factors, software as a medical device, and cybersecurity. *Biomedical Materials & Devices*, 2, 316–341. Available at: https://doi.org/10.1007/s44174-023-00113-9 (Accessed:16 May 2025).

Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the internet of medical things. *Health Policy and Technology*, 10(3), 100549. Available at: https://doi.org/10.1016/j.hlpt.2021.100549 (Accessed:16 May 2025).

Peer Response

by Fahad Abdallah - Friday, 16 May 2025, 6:50 PM

Your analysis of lethal autonomous weapon systems (LAWS) is comprehensive, impartial, and thought-provoking. You effectively emphasize the challenges of applying ethical considerations to the integration of artificial intelligence with military applications. I especially appreciate the way the discussion is framed within the context of the Q Industries example, which led to the mass resignation of engineers after the installation of lethal capabilities in its autonomous vehicles (Marsili, 2024). This case illustrates the human cost of wrongful technology choices and highlights the critical role of professionals in protecting public welfare.

Kowalczewska's (2024) analysis further supports your point, as it highlights the risks of removing human oversight from life-or-death decision-making. To support her argument, Asaro argues that such systems substantially threaten civil liberties, as governments and military bodies might abuse them. Christie et al. (2024) support this view by focusing on the professional duty to speak out when technology jeopardizes public security. The whistleblower suppression at Q Industries is a gross violation of the ACM and BCS Codes of Conduct that prioritize honesty and openness and safeguard society (O'Connell, 2023).

Your thoughts about the larger social and political ramifications of LAWS are especially thought-provoking. Panneerselvam (2024) warns that these technologies may be used exploitatively in the hands of authoritarian regimes to muzzle defiance and exert authority, which would pose a threat to democratic tenets and give rise to more global instabilities. You can fortify the analysis by using the work of the United Nations to support the development of international legal frameworks that will limit or regulate the use of LAWS (Marsili, 2024)

On the whole, your post reflects a well-debated and topical discussion on the ethical perils of autonomous weaponry. It offers important clues about why harm prevention requires ethical oversight by policymakers, engineers, and the world.

References

Christie, E. H., Ertan, A., Adomaitis, L., & others. (2024). Regulating lethal autonomous weapon systems: Exploring the challenges of explainability and traceability. *AI Ethics*, 4, 229–245. Available at: https://doi.org/10.1007/s43681-023-00261-0 (Accessed:16 May 2025).

Kowalczewska, K. (2024). Human oversight and risk-based approach to artificial intelligence: What does the Artificial Intelligence Act have in common with discussions about lethal autonomous weapon systems? *European Integration Studies*, 20(2). Available at: https://doi.org/10.46941/2024.2.8 (Accessed:16 May 2025).

Marsili, M. (2024). Lethal autonomous weapon systems: Ethical dilemmas and legal compliance in the era of military disruptive technologies. *International Journal of Robotics and Automation Technology*, 11, Article 05. Available at: https://dx.doi.org/10.31875/2409-9694.2024.11.05 (Accessed:16 May 2025).

O'Connell, M. E. (2023). Banning autonomous weapons: A legal and ethical mandate. *Ethics & International Affairs*, 37(3), 287-298. Available at: https://doi.org/10.1017/S0892679423000357 (Accessed:16 May 2025).

Panneerselvam, P. (2024). Autonomous Weapon System: Debating Legal–Ethical Considerations and Meaningful Human Control Challenges in the Military Environment. In S. Menon, S. Todariya, & T. Agerwala (Eds.), *AI, consciousness and the new humanism* (pp. [page range not provided]). Springer, Singapore. Available at: https://doi.org/10.1007/978-981-97-0503-0_12 (Accessed:16 May 2025).