Initial Post

◄ Initial Post

Display replies in nested form

Settings

Initial Post

by John Heart Ojabo - Friday, 7 February 2025, 2:14 AM

The "Medical Implant Risk Analysis" case study from ACM represents a good case for ethical analysis. In this scenario, Corazón, a medical startup developing an implantable heart health monitor with a smartphone interface, adhered to several of the ACM Code of Ethics and Professional Conduct while still failing in others (ACM, 2025).

Corazón's approach to security - encryption, bug bounty program and research - is in tandem with several ACM principles, specifically 2.9 (design and implement systems that are robustly and usably secure), 2.6 (perform work only in areas of competence) and even 3.7 (recognize and take special care of systems that become integrated into the infrastructure of society).

However, the discovery of the hard-coded initialization value vulnerability that could potentially allow nearby devices to induce a reset poses a serious ethical challenge. While Corazón and researchers have rated the risk as negligible it still touches upon the ACM ethical mandate to "avoid harm" (Principle 1.2) and underscores the ongoing need for comprehensive risk management (Principle 2.5). This also resonates with the BCS Code of Conduct's emphasis on "integrity" and "diligence," requiring members to "uphold the reputation of the profession" and "act with care and diligence in the execution of their professional duties" (BCS, 2025).

In summary, the Corazón case is a good demonstration of the inherent challenges and responsibilities of computing professionals. Both the ACM and BCS codes of conduct aims to serve as a robust framework for this professional imperatives.

REFERENCES:

ACM (2025) *ACM Code of Ethics and Professional Conduct.* Available from:https://www.acm.org/code-of-ethics [Accessed: 7 February 2025].

BCS (2025) *BCS Code of Conduct.* Available from:https://www.acm.org/code-of-ethics [Accessed: 7 February 2025].

Permalink Reply

Peer Response

by Oi Lam Siu - Sunday, 9 February 2025, 8:11 AM

Hi John,

Thank you for this well-structured analysis of the Corazón case (ACM, n.d.). I agree that the startup demonstrates commendable alignment with the ACM principles on security (e.g. Principle 2.9) and competence (Principle 2.6), as well as the broader importance of handling systems deeply integrated into society (Principle 3.7) (ACM, 2018). The bug bounty programme and the open engagement with researchers highlight Corazón's proactive stance on transparency and risk mitigation. However, the hard-coded initialization value, despite being rated as "low risk", does indeed raise ethical concerns under "avoid harm" of ACM Principle 1.2 (ACM, 2018). Even a small vulnerability in a healthcare device can potentially compromise patient confidence, underlining the continuous nature of risk assessment in medical technologies (Halperin et al, 2008).

Moreover, your observation about the BCS Code of Conduct's focus on "integrity" and "diligence" is particularly relevant. The BCS stipulates that professionals should act responsibly to maintain the public's trust and uphold the profession's reputation (BCS, 2022). In this context, swiftly addressing the vulnerability, informing stakeholders, and regularly reviewing sy become central responsibilities.

Overall, your post offers a salient reminder that even robust security processes require continuous evaluation and improvement, especially in life-critical systems. The Corazón scenario exemplifies how small oversights may undermine wider confidence in emerging healthcare technologies—even when the ethical code has largely been followed.

Best regards

Helen

References

ACM (2018). ACM Code of Ethics and Professional Conduct. Available from: https://www.acm.org/code-of-ethics [Accessed 1 February 2025].

ACM (n.d.) Case Study: Medical Implant Risk Analysis. Available at: https://www.acm.org/code-of-ethics/case-studies/medical-implant-risk-analysis [Accessed 9 February 2025].

BCS (2022). BCS Code of Conduct. Available from: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct [Accessed 1 February 2025].

Halperin, D. et al. (2008) 'Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses', 2008 IEEE Symposium on Security and Privacy. Oakland, California, 18–21 May. IEEE. 129–142.

Permalink **Show parent** **Edit** **Delete** **Reply**

◄ **Initial Post**