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 revealing the complexities and potential pitfalls in navigating ethical considerations by still failing in others (ACM Case Study, 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) (ACM, 2018).

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). As already highlighted by peer feedback, even a small vulnerability in a medical device can erode patient confidence, emphasizing the need for continuous risk assessment, especially in life-critical systems (Halperin et al., 2008). 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).

Furthermore, the case raises critical questions about transparency and risk disclosure. While Corazón may have followed industry best practices, their decision to downplay the severity of the vulnerability raises concerns under Principle 1.3 (be honest and trustworthy) which underscore the ethical obligation of full disclosure.

In summary, the Corazón case is a good demonstration of the inherent challenges and responsibilities of computing professionals. It is a powerful reminder that ethical considerations in computing are multifaceted and ongoing. Both the ACM Code of Ethics and BCS Codes of Conduct aims to serve as a robust framework for this professional imperatives.

REFERENCES:

ACM (2018) *ACM Code of Ethics and Professional Conduct.* Available from:

https://www.acm.org/code-of-ethics   [Accessed: 16 February 2025].

ACM Case Study (2025) Case Study: Medical Implant Risk Analysis. Available at:

https://www.acm.org/code-of-ethics/case-studies/medical-implant-risk-analysis

[Accessed 16 February 2025].

BCS (2025) *BCS Code of Conduct.* Available from:

https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-cond

uct/   [Accessed: 16 February 2025].

Halperin, D., Heymann, T., Keromytis, A. D., & Preneel, B. (2008). Security and privacy

in implantable medical devices. *IEEE Pervasive Computing*, 7(1), 30-39.