Initial Post

The *Corazón* case study from the Association for Computing Machinery (ACM, 2018) presents a fictional yet realistic scenario illustrating how ethical principles apply to emerging medical technologies. It concerns a startup that developed an implantable heart-monitoring device connected to a smartphone application. After release, an independent researcher discovered a flaw that allowed nearby devices to send reset commands to the implant. While the case is not real, it serves as an educational example for evaluating professional and ethical conduct in computing.

The case underscores the need to balance the benefits of wireless medical technology with its potential dangers. Wireless connectivity in implantable medical devices (IMDs) enables real-time health monitoring and life-saving interventions but also exposes patients to risks of malfunction, data theft, or malicious interference (Camara, Peris-Lopez and Tapiador, 2015). Pycroft et al. (2018) similarly warn that the growing reliance on connected devices increases vulnerability to cyberattacks and system failures, which can lead to harm or erode public trust in medical innovation.

From an ethical perspective, the ACM Code of Ethics requires professionals to "avoid harm" and ensure systems are "robustly and comprehensively tested" (ACM, 2018). *Corazón's* cooperation with researchers and transparent bug-bounty programme reflect this duty and demonstrate ethical accountability. The British Computer Society (BCS, 2025) Code of Conduct likewise emphasises the *Public Interest* and *Professional Competence and Integrity*, urging practitioners to protect health, respect privacy, and continually update their technical knowledge.

Ultimately, the *Corazón* case highlights that ethical computing in healthcare is not only about compliance but about judicious balance. Professionals must weigh the potential benefits of wireless medical innovation with the dangers of misuse or malfunction, maintaining transparency, collaboration, and continuous improvement to protect both life and data.

References

Association for Computing Machinery (2018) *ACM Code of Ethics and Professional Conduct: Case Studies – Medical Implant Risk Analysis.* Available at: **https://ethics.acm.org/code-of-ethics/case-studies/medical-implant-risk-analysis/**

Association for Computing Machinery (2018) *ACM Code of Ethics and Professional Conduct.* Available at: https://www.acm.org/code-of-ethics

British Computer Society (2025) *BCS Code of Conduct.* Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/

Camara, C., Peris-Lopez, P. and Tapiador, J. E. (2015) 'Security and privacy issues in implantable medical devices: A comprehensive survey', *Journal of Biomedical Informatics,*

Pycroft, L., et al. (2018) 'Security of implantable medical devices with wireless communication', *Health Information Management Journal*