Initial post - Codes of Ethics and Professional Conduct

The Corazón case study (Association for Computing Machinery, 2025) demonstrates both adherence to and potential violations of professional computing ethics when examined against the BCS Code of Conduct (British Computing Society, 2022). While the company's charitable initiatives align with BCS Section 1.1 regarding public interest and promoting equal access to IT benefits, critical concerns emerge regarding professional competence and duty to relevant authorities.

The hard-coded initialization value represents a fundamental security flaw that potentially violates BCS Section 2.1, which mandates undertaking only work within professional competence. Medical device security requires specialized expertise, and this vulnerability suggests inadequate security architecture. The researcher's ability to demonstrate device manipulation contradicts BCS Section 1.1's requirement for "due regard for public health, privacy, security and wellbeing."

Legally, medical device regulations across jurisdictions require robust cybersecurity frameworks. The FDA's 2025 cybersecurity guidance mandates secure design principles, while the EU's Medical Device Regulation (MDR 2017/745) emphasizes risk management throughout device lifecycles (European Union, 2017; US Food and Drug Administration, 2025). The vulnerability could constitute regulatory non-compliance, exposing Corazón to significant liability.

The company's responsive collaboration with researchers demonstrates adherence to BCS Section 2.5 regarding honest criticism acceptance. However, the dismissal of risk as "negligible" without comprehensive impact assessment potentially violates professional responsibility standards. Computing professionals must prioritize patient safety over commercial considerations, ensuring thorough vulnerability remediation rather than risk minimization.

References:

Association for Computing Machinery (2025) *Case Study: Medical Implant Risk Analysis*. Available at: https://www.acm.org/code-of-ethics/case-studies/medical-implant-risk-analysis (Accessed: 31 of August 2025).

British Computing Society (2022) *BCS Code of Conduct for members - Ethics for IT professionals*. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct (Accessed: 31 of August 2025).

European Union (2017) *Regulation - 2017/745 - EN - Medical Device Regulation - EUR-Lex*. Available at: https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng (Accessed: 31 of August 2025).

US Food and Drug Administration (2025) *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*. FDA. Available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions (Accessed: 31 of August 2025).