Initial Post

The Corazón case is a strong example of ethical practice in computing, showing clear links to both the ACM Code of Ethics and the BCS Code of Conduct (ACM, 2018b). The company's emphasis on user privacy and wellbeing is evident through its use of encryption and short-range wireless communication, which help protect sensitive patient data. These choices support the responsibility to safeguard public health and privacy, as outlined in ACM Principle 1.1 and BCS Rule 1.1 (ACM, 2018; BCS, 2021).

Corazón's approval from medical regulators across several countries shows that the company takes legal compliance seriously, aligning with ACM Principle 2.3 and BCS Rule 2.4. That said, a security flaw discovered by a researcher—caused by predictable wireless behaviour—raises concerns. Even if the risk is small, it could allow future interference with the device or data. Given that the system handles health data, classified as special category data under the UK GDPR, this could be serious. Article 32 of the UK GDPR requires organisations to implement appropriate security measures to protect personal data, while Article 5(2) places a clear obligation on them to demonstrate ongoing compliance with these requirements (UK Government, 2016). However, as Moor (2005) argues, emerging technologies often develop faster than regulation, creating policy vacuums that place additional ethical responsibility on computing professionals. In such contexts, legal compliance alone may be insufficient; designers must actively anticipate potential harms and apply ethical judgement in the absence of clear rules.

Socially, Corazón has made a positive impact by working with charities to improve access for patients from disadvantaged backgrounds. This aligns with ACM Principle 1.4 and BCS Rule 1.4, which promote inclusion and equal access to technology (ACM, 2018; BCS, 2021).

Professionally, Corazón responded responsibly by working with the researcher to assess the risk. This shows openness, competence, and integrity, consistent with ACM Principles 2.5 and 2.6 and BCS Rules 2.1 and 2.5 (ACM, 2018; BCS, 2021).

Overall, while Corazón meets many ethical and professional expectations, this case highlights the ongoing need for secure design and careful risk management in healthcare technologies.

References:

ACM, (2018). ACM Code of Ethics and Professional Conduct. Association for Computing Machinery. Available at: https://www.acm.org/code-of-ethics (Accessed 5 May 2025).

ACM, (2018b). Case Study: Medical Implant Risk Analysis. Association for Computing Machinery. Available at: https://www.acm.org/code-of-ethics/case-studies/medical-implant-risk-analysis (Accessed 5 May 2025).

BCS, (2021). BCS Code of Conduct. British Computer Society. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/ (Accessed 5 May 2025).

Moor, J.H., (2005). Why we need better ethics for emerging technologies. Ethics and Information Technology, 7(3), pp.111–119. Available at: https://link.springer.com/article/10.1007/s10676-006-0008-0 (Accessed 5 May 2025).

UK Government, (2016). General Data Protection Regulation (EU) 2016/679. Available at: https://www.legislation.gov.uk/eur/2016/679/contents (Accessed 5 May 2025).