Summary post

My initial analysis of the Corazón case study focused on the tension between the company's positive security practices and the critical flaw of dismissing a discovered vulnerability as "negligible" without comprehensive impact assessment. I argued that while Corazón demonstrated regulatory compliance and researcher collaboration, their risk minimization approach potentially violated BCS Code requirements for professional competence and public interest protection, emphasizing that professional judgment must prioritize patient safety over commercial considerations (British Computing Society, 2022).

Parallel discussions on other students' posts significantly reinforced my central arguments. Yousif's analysis supported my emphasis on regulatory compliance and proactive security practices. Julius and Dalbir's contributions questioned whether risk-based approaches are ethically acceptable in life-critical systems. Kieron's comprehensive analysis directly addressed my concerns about "negligible risk" assessments, arguing such terminology is inappropriate for medical devices where even low-probability vulnerabilities can have severe consequences (Williams and Woodward, 2015). Valentina argued that "negligible" risk is "almost unacceptable" in medical contexts, while Mihail suggested replacing "negligible" with "non-zero" risk terminology, citing research showing that software flaws in implantable devices can lead to direct malfunctions, patient anxiety, and health risks (Halperin *et al.*, 2008). This aligns with calls for security-by-design approaches in medical technologies (Maisel and Kohno, 2010).

The collective discussion demonstrates strong convergence around the principle that medical device computing requires fundamentally different ethical standards than general computing applications. The consensus confirms that professional ethics in healthcare technology must prioritize comprehensive vulnerability remediation over cost considerations or optimistic risk assessments, reinforcing that computing professionals in medical contexts bear heightened responsibility for patient safety.

References:

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 August 2025).

Halperin, D. *et al.* (2008) 'Security and Privacy for Implantable Medical Devices', *IEEE Pervasive Computing*, 7(1), pp. 30–39. Available at: https://doi.org/10.1109/MPRV.2008.16.

Maisel, W.H. and Kohno, T. (2010) 'Improving the Security and Privacy of Implantable Medical Devices', *New England Journal of Medicine*, 362(13), pp. 1164–1166. Available at: https://doi.org/10.1056/NEJMp1000745.

Williams, P.A. and Woodward, A.J. (2015) 'Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem', *Medical Devices (Auckland, N.Z.)*, 8, pp. 305–316. Available at: https://doi.org/10.2147/MDER.S50048.