Summary Post

Thank you all for the engaging discussion around the Corazón case. It is clear this example offers not only strong ethical practices but also critical lessons in proactive risk management and design accountability in computing.

As highlighted, Corazón shows commendable alignment with the ACM Code of Ethics and BCS Code of Conduct, particularly in prioritising user privacy, regulatory compliance, and social inclusion. Its use of encryption and wireless constraints reflects ethical awareness (ACM 1.1, BCS 1.1), and its outreach efforts promote equal access to technology (ACM 1.4, BCS 1.4).

However, the case also underscores that compliance is not the same as security. The discovered vulnerability in wireless behaviour, although minor, raises significant concerns in a system handling special category data under the UK GDPR (UK Government, 2016). As several of you pointed out, this demonstrates the need for proactive risk assessment and anticipatory design, especially in life-critical technologies. Dhia and Koulthoum rightly emphasise that ethical responsibility often extends beyond legal compliance, and Sedenberg and Hoffmann's (2016) concept of anticipatory governance strengthens this argument.

Moreover, Jaafar's point about ethics being a "moving target" is particularly relevant. As technology evolves faster than regulation (Moor, 2005), the burden increasingly falls on professionals to apply judgement and foresight. Greater transparency, ongoing security updates, and practices like external penetration testing (as Koulthoum suggests) could help mitigate risks and build public trust.

These insights collectively highlight the complex responsibilities facing computing professionals working with sensitive systems.

In conclusion, while Corazón demonstrates many ethical strengths, it also exemplifies the continuous and dynamic nature of ethical responsibility in computing. Especially in healthcare, a sector where the stakes are high, secure design, anticipatory risk management, and ongoing accountability must remain central.

References:

ACM, (2018). *ACM Code of Ethics and Professional Conduct*. Association for Computing Machinery. Available at https://www.acm.org/code-of-ethics (Accessed 15 July 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 15 July 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 15 July 2025)

Sedenberg, E. and Hoffmann, A.L., (2016). *Recovering the history of informed consent for data science and internet industry research ethics*. arXiv preprint arXiv:1609.03266. Available at: https://arxiv.org/abs/1609.03266 (Accessed 15 July 2025)

UK Government, (2016). *General Data Protection Regulation (EU) 2016/679*. Available at: https://www.legislation.gov.uk/eur/2016/679/contents (Accessed 15 July 2025)