Collaborative Discussion 1: Peer Response 3 (276 words)

Hi Panagiotis,

Thank you for your contribution to the discussion posting.

Your initial post generally presents a balanced view on the company's handling of a security vulnerability in their medical implant system, highlighting the proactive measures the company has embedded within their practices. Data encryption, the bug bounty program, alongside their charitable work are key in underpinning ethical principles. However, the analysis acknowledges the potential legal liabilities arising from exploits of the hard-coded value and appropriately emphasises the need for ongoing collaboration with security experts to resolve the issue.

The discussion could benefit from a more explicit consideration of the regulatory landscape governing medical devices, and data security and protection. The hard-coded value is a significant security smell (Rahman et al., 2019), and despite the current negligible outcome, it should not be discredited, as may indicate risk of further security smells present in the code. Additionally, while data encryption is mentioned, specific regulations like the Health Insurance Portability and Accountability Act (HIPAA) (in the US), General Data Protection Regulation (GDPR) (in Europe), and other relevant data privacy laws are not discussed. For example, it is recognised that HIPAA is not fully sufficient to regulate medical devices (Maisel, 2010), therefore it remits further discussion on how medical devices and data processed by these devices should be protected. The Medical Devices Regulation (MDR) in Europe targets this (Saint-Gobain, n.d.), and it imposes stringent requirements for safety,

efficacy, and post-market surveillance. Overall, addressing these regulations would provide a more comprehensive view of Corazon's responsibilities and potential liabilities.

Thanks again for your contribution, it was interesting to assess a more positive example in the context of the topic of discussion.

References:

Maisel, W.H. (2010) Improving the security and privacy of implantable medical devices. *The New England journal of medicine*, *362*(13): 1164.

Rahman, A., Parnin, C. & Williams, L. (2019) The seven sins: Security smells in infrastructure as code scripts. In *2019 IEEE/ACM 41st International Conference on Software Engineering (ICSE)* (164-175). IEEE.

Saint-Gobain (n.d.) What is EU MDR and Why is it Necessary? Saint-Gobain. Available from: https://www.medical.saint-gobain.com/resources/blog/eu-mdr-what-it-and-why-it-necessary [Accessed 6 February 2025]