Peer Response

Hi Danielle,

That's a great summary of the case study!

Whilst I agree that Corazon showcased great commitment to many of ACM's principles by collaborating with the researcher to identify the risk this vulnerability proposed, I did question whether this risk classification should have been carried out independently instead.

The ACM (2024) case study states that the hardcoded value "created a predictable pattern in the data exchanges that could be manipulated," which sounds quite severe. Corazon will naturally have a biased view and potential conflict of interest in addressing vulnerabilities, particularly if they would be challenging to implement, which the case study suggests would be the case. It also mentions that "there is insufficient evidence at this point to determine the scope of the risk induced by this design." To me, it sounds like more could have been done to better appraise the risk, considering its potential impact on the users of these medical devices.

BCS (2024) principle 1.1 argues that technologies should be developed with "due regard for public health, privacy, security and wellbeing of others" - do you think this is reflected in how the vulnerability was investigated and classified? Do you have any thoughts of how such vulnerabilities should be classified in the future? Do you believe that the users of such devices should have a say in such classifications?

Best wishes,
Dom

References

Association for Computing Machinery (ACM), 2024. *Case Study: Medical Implant Risk Analysis*. Available at: https://ethics.acm.org/code-of-ethics/using-the-code/case-medical-implant-risk-analysis/ [Accessed 19 August 2024].

British Computer Society (BCS), 2024. *BCS Code of Conduct*. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/ [Accessed 19 August 2024].