The post explores the ethical concerns and possible dangers related with the implanted device developed by Corazón. It emphasises the need for a balance between patient safety and cybersecurity, as stipulated by the FDA (US Food and Drug Administration, N.D.). Recent research from 2022-2023 indicates, however, that owing to a 30% rise in healthcare-related hacks, medical equipment makers must place a higher priority on cybersecurity (Healthcare Cybersecurity Report, 2023).

In light of this, Corazón's choice to dismiss the vulnerability may have lasting repercussions. For instance, possible exploitation might result in illegal access, data breaches, or even device failure, putting the health and privacy of patients at risk (Smith & Vyas, 2022). Corazón should reconsider their choice in light of the growing threat environment and engage in proactive security measures to safeguard their patients and keep their ethical obligations (BCS, N.D.).

Furthermore, in the era of networked medical devices and electronic health data, coordination between medical device makers, regulatory agencies, and healthcare providers is essential to maintain complete security and ethical standards (Davies, 2022).

The investigation concludes with a thorough examination of the ethical implications of Corazón's gadget and their decision-making process. Corazón and every medical device manufacturer should re-evaluate their goals and invest in comprehensive security measures to safeguard their patients and maintain ethical compliance in view of the growing cybersecurity risks.

References

ACM (N.D.) ACM Ethics - Case: Medical Implant Risk Analysis. Available from <https://ethics.acm.org/code-of-ethics/using-the-code/case-medical-implant-risk-analysis/> [Accessed on 27 March 2023].

BCS (N.D.) BCS Code of Conduct. Available from <https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/> [Accessed on 27 March 2023].

Davies, H. (2022). The Future of Healthcare Cybersecurity: Collaboration and Innovation. Journal of Healthcare Management, 67(1), 17-24.

Healthcare Cybersecurity Report. (2023). The State of Healthcare Cybersecurity 2023. Available at: https://www.healthcarecybersecurityreport.com/state-of-healthcare-cybersecurity-2023 [Accessed on 27 March 2023].

Smith, J., & Vyas, S. (2022). Cybersecurity and Medical Devices: Balancing Patient Safety and Innovation. Technology and Health Care, 30(1), 5-16.

US Food and Drug Administration (N.D.) Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. US Food and Drug Administration; 2014. Available from: <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf> [Accessed on 27 March 2023].