Hello Mohammed,  
  
Thank you for bringing another insight to the medical implant’s technology case by emphasizing the importance of cybersecurity of medical implant device and the failure to comply with the measures could lead to severe harm or even loss of life. Also, the reference to the legal obligations such as enforcement of stringent testing, transparency, and data security standards as guided by the regulation of medical devices in Great Britain (Gov.uk, 2021) is on point. Addition to the point on cybersecurity of the device, the risks associated with cybersecurity threats and vulnerabilities should be considered throughout all stages in the life of a medical device, from development through end of support (EOS) and there should be cybersecurity risk management in place (International Medical Devic Regulator Forum,2023). Corazon complied with this best practice by having an open bug bounty program inviting disclosure of potential vulnerabilities in their app (Association for Computing Machinery).  
  
Furthermore, the implant medical technology is an example of Healthcare Internet of Things (IoT)devices, and the device do collects and stores sensitive patient information which any vulnerabilities in the device may lead to data breaches, exposing health records, personal information, and medical histories to an unauthorized individual. This challenge could result to legal and privacy-related repercussions as it contravenes GDPR policy and could attracts penalties (Rashid.M, et. al ,2024).  
  
Conclusion  
Compliance by the rules and laws guiding any ethical codes and professional conduct has a long-term benefit to any organisation such as continuity in business, avoiding any penalties or reputational risk and minimization of vulnerabilities of any kind.  
  
Thank you.  
Njide  
  
Reference:  
Association for Computing Machinery (2018) ACM Code of Ethics and Professional Conduct. Available from: https://ethics.acm.org/ [Accessed: 28 August 2024].  
  
Association for Computing Machinery (N.D.) Case: Medical Implant Risk Analysis. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/ [Accessed: 28 August 2024].  
  
International Medical Devic Regulator Forum (2023).Principles and Practices for the Cybersecurity of Legacy Medical Devices. Available from: https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices [Accessed 3rd September 2024].  
  
Rashid.M, et, al (2024). European Journal of Electrical Engineering &Computer Science. IoT Complexity: Security, Vulnerabilities and Risks. Vol.8 No. 1. Available from: https://www.ejece.org/index.php/ejece/article/view/597 [Accessed 3rd September 2024)  
  
British Computer Society (BCS), 2022. BCS Code of Conduct. Available from: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/ [Accessed 28 August 2024].