Review case: Medical Implant Risk Analysis (Coraźon)

Coraźon is a medical technology that develops implantable medical devices. Their product provides monitoring and controlling the device using a smartphone application.

The General Data Protection Regulation of the European Union prescribes that privacy and confidentiality of data must be protected when data is in transit(exchanged or transmitted) and when information is at rest(stored)(Pikulik, 2019). Coraźon's practice of employing cryptographic algorithms on data exchanged between the device and the smartphone and encrypting stored data on the smartphone demonstrates compliance with the British Computer Society (BCS) code of conduct. Their practice show adherence to BCS code 1. A (Public interest: regard for privacy, security and wellbeing of others) and code 2d (Professional Competence and Integrity: knowledge and understanding of the legislation and ensuring compliance when practising professional responsibilities). The employed cryptographic algorithms protect the privacy and confidentiality of the exchanged information from eavesdropping and man-in-the-middle attack techniques. Applying state of the art encryption on the stored data ensures that data confidentiality is protected against unauthorised access if the smartphone is lost or stolen.

The degree to which an organisation can manage risk is closely coupled to the success of the entity or product that is the object of risk assessment (Hohan et al., 2015). Risk management is a component of continuous improvement. The intertwining of these two disciplines creates an opportunity for a proactive elimination of potential sources of threats and failures, which is in contrast to the reactive approach through the control of variables (Acartürk et al., 2021). Through the open bug bounty program, Coraźon demonstrated commitment to continuous improvement and risk management. Their dedication shows compliance with code 2c (Develop your professional knowledge, skills and competence on continuos bases). Through consultation with the independent researcher regarding the vulnerability discovered by the researcher, they have demonstrated an openness to alternative views and constructive criticism in their endeavour to improve continuously. They have committed to comply with code 2e of BCS(Of et al., 2021).

Bibliography :

Acartürk, C., Ulubay, M., & Erdur, E. (2021). Continuous improvement on maturity and capability of Security Operation Centres. *IET Information Security*, *15*(1), 59–75. https://doi.org/10.1049/ise2.12005

Hohan, A. I., Olaru, M., & Pirnea, I. C. (2015). Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles. *Procedia Economics and Finance*, *32*(15), 352–359. https://doi.org/10.1016/s2212-5671(15)01404-5

Of, C., For, C., & Members, B. C. S. (2021). *Correspondence in connection with this Code of Conduct should be directed to : Customer Service team BCS , The Chartered Institute for IT , 3 Newbridge Square Swindon Email : custsupport@bcs.uk*. *June*, 5–9.

Pikulik, T. (2019). Gdpr Compliant Methods of Data Protection. *6th SWS International Scientific Conference on Social Sciences ISCSS 2019*, *2*(March). https://doi.org/10.5593/sws.iscss.2019.2/s05.069