

# Research Methods and Professional Practice January 2022

[Home](#) / / [My courses](#) / / [RMPP\\_PCOM7E January 2022](#) / / [Unit 1](#) / / [Collaborative Learning Discussion 1](#) /  
/ [Initial Post](#) /

## « Collaborative Learning Discussion 1



Samuel Tselapedi

### Initial Post

1 day ago

1 reply



Last 10 mins ago

### Review case: Medical Implant Risk Analysis (Corazón)

Corazón 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). Corazón'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, Corazón demonstrated commitment to continuous improvement and risk management. Their dedication shows compliance with code 2c (Develop your professional knowledge, skills and competence on continuous 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](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 ISCSSL 2019*, 2(March).

<https://doi.org/10.5593/sws.iscsl.2019.2/s05.069>

Reply

## 1 reply

1



Post by [Jan Kufner](#)

[10 mins ago](#)

peer response

To have a hard coded initialization value that creates predictable patterns in a way that encryption can be broken is not state of the art. Transport Layer Security (TLS) offers many ways to implement secure authentication and encryption between devices. The company also stated that the risk of harm is negligible after the exploit got published by the security researcher. I would argue that deletion of detected heart failures from memory can lead to severe consequences for individuals. This rationale to not improve the issues detected can therefore not be followed, since state of the art technology (TLS) is available to mitigate and since the severity to patients is underrated by the company. I would argue that the start up either claims a level of competency in cyber security for implants that they do not have or that they have disregard for public health. BCS (2021)

### References

BCS (2021) Code of Conduct for BCS Members. Available from: <https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf> [Accessed 25 January 2022].

Reply

[Edit](#) [Delete](#)

Maximum rating: -

Add your reply



Your subject



Type your post

Dateien auswählen

Keine ausgewählt

Submit

Use advanced editor and additional options

OLDER DISCUSSION

[Initial Post](#)

NEWER DISCUSSION

[Initial Post](#)

