# Research Methods and Professional Practice June 2023

## Collaborative Learning Discussion 1

## Initial Post

Settings

◄ Initial Post    Summary Post ►

Display replies in nested form

**Initial Post**

by Beatrice Mutegi - Saturday, 24 June 2023, 3:30 AM

**ACM Code of Ethics Case Study: Medical Implant Risk Analysis**

(ACM, 2018) describes The Association of Computing Machinery (ACM) Code of Ethics and Professional Practice as a guide that helps computing professional make ethica decisions and prioritize the public good.
(ACM, N.D) describes a case study on Corazón, a medical technology startup that implemented an open bug bounty program for their implantable heart health monitoring device app. This study highlighted the ACM Code of Ethics (ACM Code 2018 Task Force, 2018) that Corazón's aligned with, which includes:

- Principle 1.1: Contribution to society and human well-being by providing accessibility to their heart health monitoring devices.
- Principle 2.3: Adhering to medical device regulations by ensuring that their product is safe and efficient.
- Principle 2.5: Evaluated their systems for any impacts and risks by consulting with the researcher.
- Principle 2.6: Showed competence by using standard cryptographic algorithms instead of unproven proprietary techniques.
- Principle 2.9: Displayed dedication to designing a robust and secure systems by implementing an open bug bounty program to identify overlooked risks and vulnerabilities.
- Principle 3.7: Integrated their system into the society by collaborating with charities so as to provide their services to the less unfortunate people in the society.

Moreover, impacts on the legal, social issues and professionalism of the computing professionals involved include:

- Legal: Corazón's adherence to Principle 2.3 by ensuring that their product meets the medical device regulations and standards for safety and efficacy.
- Social: Corazón ensured that their services were accessible to all, the poor and the rich in the society.
- Corazon's computing professionals demonstrated professionalism by:

  o Following ethical principles in their product development, security practices, and risk analysis.
  o Their collaboration with independent researchers and promptly addressing potential vulnerabilities.
  o By prioritizing a thorough risk analysis and mitigating the identified risks and vulnerabilities swiftly.

ACM's comparison to British Computer Society (BCS) Code of Conduct include:

- Both serve as code of ethics to IT professionals and they work towards making IT for everyone e.g., promoting equal accessibility of IT benefits to everyone in the society (Trustee Board, 2022).
- BCS serves specifically in the UK and the members are forbidden to misrepresent the organization while ACM Code is global (Oz, 1992).

**References**

ACM Code 2018 Task Force, 2018. *ACM Code of Ethics and Professional Conduct.* [Online]
Available at: https://www.acm.org/code-of-ethics
[Accessed 21 June 2023].

ACM, 2018. *ACM Code of Ethics and Professional Conduct.* [Online]
Available at: https://www.acm.org/code-of-ethics/case-studies
[Accessed 21 June 2023].

ACM, N.D. *Case: Medical Implant Risk Analysis.* [Online]
Available at: https://ethics.acm.org/code-of-ethics/using-the-code/case-medical-implant-risk-analysis/
[Accessed 21 June 2023].

Oz, E., 1992. Ethical Standards for Information Systems Professionals: A Case for a Unified Code.. *MIS Quarterly,* 16(4), pp. 423-433.

Trustee Board, 2022. *COde of Conduct for BCS Members.* [Online]
Available at: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf
[Accessed 21 June 2023].

Knowledge Base

Permalink Reply

**Peer Response**

by Laura Saxton - Saturday, 24 June 2023, 10:33 AM

Beatrice, thank you for this very informative and well-structured post. You showcase succinctly and clearly all that Corazón is doing correctly as a company to comply with the regulations set out by ACM (n.d.) and BCS (2022). One ethical code the company may not be in full compliance with, however, is BCS 2.f., which states stakeholders must “avoid injuring others [...] by false or malicious or negligent action or inaction” (BCS, 2022: 2).

Security gaps in medical devices similar to Corazón’s have been reported, which resulted both in the implementation comprehensive security patches (Fu & Kramer, 2017) and increased governmental regulations (Voelker, 2018) to safeguard patient security. In addition, hard-wired connections like the one Corazón devices have can “compromise protected health information” (Stern, 2016: 465), with hard-coded and/or factory setting values as documented facilitators of breach (Pinto & Stuttard, 2011).

I wonder, since issues with Industry 4.0 medical device security have been reported in major medical markets, and the Corazón devices have a well-known security flaw in the wireless connectivity protocol, how this effects the company’s ethical compliance, in your opinion?

Thank you again for a very engaging post.

References

ACM (n.d.) *Case: Medical Implant Risk Analysis.* [Online] Available at: https://ethics.acm.org/code-of-ethics/using-the-code/case-medical-implant-risk-analysis/

BCS (2022) Code of Conduct for BCS Members. [online] Available at: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf

Fu, K. & Kramer, D. B. (2017) Cyber Security concerns and Medical Devices: Lessons From a Pacemaker Advisory. *JAMA*, 318 (21): 2077 - 2078

Pinto, M. & Stuttard, D. (2011) The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws. 2nd Ed. Indianapolis, USA: Wiley.

Stern, G, (2016) A Life Cycle Approach to Medical Device Cybersecurity. *Biomedical Instrumentation & Technology*. AAMI: 464 - 466

Voelker, R. (2018) FDA Joins New Effort to Strengthen Medical Device Cybersecurity. *JAMA*, 320 (19): 1970

Permalink Show parent Reply

**Peer response**

by Hamad Ahmad - Wednesday, 28 June 2023, 12:31 PM

Thank you for sharing this insightful analysis of the ACM code of ethics through the lens of Corazon’s study case. I appreciate the methodology you have used and compared the case from both the ACM and British computer society.

I would like to add a few points for further consideration:

1. Multidisciplinary Collaboration: to complement any independent research, it may be of more value for Corazon to collaborate with professionals from various disciplines such as medicine, law, and ethics. Van Wynsberghe (2013) notes such collaborations in medical technology can be valuable to a more comprehensive understanding of managing potential risks.

2. Patient Data Protection: Principle 1.6 of the ACM code discuss the concept of privacy (ACM, 2018). In the context of medical implants, the patient's data confidentiality is important and shouldn’t be compromised (Kramer et al., 2012). It would be interesting to me personally to analyse how Corazon addresses this aspect.

3. Ongoing or continuous risk management: while Corazon opened a bug bounty program is a proactive measure, a reactive approach with ongoing iterations of managing risks would have been of greater value ( Levenson & Turner, 1993). And I would also be interested a framework that proposes the process for this case though it would have been overkill for this discussion.

Overall, your post provides an excellent complete overview of the ethical considerations in the development of medical implant technologies. Adding these extra dimensions would make the analysis more robust if it wasn’t for the word limit count.

**References**:

ACM. (2018). ACM Code of Ethics and Professional Conduct. https://www.acm.org/code-of-ethics

Kramer, D. B., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K., & Reynolds, M. R. (2012). Security and privacy qualities of medical devices: An analysis of FDA postmarket surveillance. PloS one, 7(7), e40200.

Leveson, N. G., & Turner, C. S. (1993). An investigation of the Therac-25 accidents. Computer, 26(7), 18-41.

Van Wynsberghe, A. (2013). Designing robots for care: Care centered value-sensitive design. Science and engineering ethics, 19(2), 407-433.

Permalink Show parent Reply

**Re: Initial Post**

by Mahamad Ibrahim - Wednesday, 28 June 2023, 6:09 PM

The continuous enhancement of quality of life and society through technology is undeniable, which leads to human well-being. Furthermore, the immense access to information provided a large number of opportunities for innovators to initiate ideas that contribute to solving complex problems (Deb, 2014). By implication, Corazon’s implantable heart health monitoring device application is facilitating physicians’ ability to make necessary medical decisions more efficiently by gathering relevant information, as the device reports the patient’s health status immediately.

Considering the nature of information stored and processed by Corazon's application (health information), security concerns of what approaches and measures are set in place to protect such sensitive information. According to the case study, Corazon implemented cryptographic methods to secure the information. (ACM, N.D). on the contrary, cryptographic standard still have some open issues when it comes to implementation. Soomro et al. (2019) highlighted some of the issues such as high cost of implementing these methods, the performance of the cryptographic standards, and many more.

On the other hand, to keep security posture up to date and remediate existing vulnerabilities, Corazon started a bug bounty program for researchers to help in identifying and reporting vulnerabilities in the application. Money is a crucial motivator for cybersecurity experts to make contributions to help organizations finding vulnerabilities. According to Walshe & Simpson2020, the number of bug bounty programs available on Hackerone website increased from 82 to 212 since 2015. By implication, this saves a huge amount of money for Corazon's cybersecurity budget.

From another perspective, some cons of such programs are assumable by considering the involvement of third parties in the application (bug bounty researchers in Corazon's case) might raise the alarm of accessing and sharing sensitive medical information in case a researcher found a vulnerability and did not report. As the possibility of disclosing information by researchers exists, organizations tend to establish legal measures to minimize and eliminate any public exposure of their data (Hamper, 2020).

Deb, S. (2014) Information Technology, Its Impact on Society, and Its Future. Advances in Computing 4(1): 25-29 doi:10.5923/j.ac.20140401.07

Soomro, S. Belgaum, M. Alansari, Z. Jain, R. (2019) 'Review and Open issues of Cryptographic Algorithms in Cyber Security', International Conference on Computing: Electronics & Communications Engineering (iCCECE), 2019. London: IEEE. 158-162.

Walshe, T. and A. Simpson, A. (2020) 'An Empirical Study of Bug Bounty Programs', 2nd International Workshop on Intelligent Bug Fixing (IBF). London, ON, Canada, 2020. London: IEEE. 35-44.

Hamper, R. (2020) Software bug bounties and the legal risks to security researchers. Available from:https://unsworks.unsw.edu.au/entities/publication/603c7b44-138d-4178-8162-d9776a765a13 [Accessed 27 June 2018]

ACM. (n.d) Medical Implant Risk Analysis - ACM Ethics. Available at: https://ethics.acm.org/code-of-ethics/using-the-code/case-medical-implant-risk-analysis/ [Accessed on 27th June 2023]

Permalink Show parent Reply

◄ Initial Post

Summary Post ►