Case Study: Medical Implant Risk Analysis

The Association of Computing Machinery (ACM) Code of Ethics and Professional Practice serves computing professionals by helping them make ethical decisions and prioritize the public good (ACM, 2018). My initial post focused on one of the ACM case studies, Medical Implant Risk Analysis, whereby, Corazón, a medical technology startup, implemented an open bug bounty program for their implantable heart health monitoring device app (ACM, N.D). Corazón's actions aligned with several ACM Code of Ethics principles that resulted to impacts such as:

- Legal, whereby Corazón aligned with:
    - Principle 2.3 by ensuring compliancy with regulations and standards of governmental agencies, such as: Data privacy (ACM, N.D) (ACM, 2018).
- Social, whereby Corazón aligned with:
    - Principle 1.1 of the ACM Code by partnering with numerous charities to ensure accessibility and affordability of their services to all patients, both rich and poor (ACM, N.D) (ACM, 2018).
- Professionalism, whereby Corazón aligned with:
    - Principle 2.6 and 2.9 of the ACM Code by showing competence and commitment to design robust and secure systems with the use of standard cryptographic algorithms, data encryption, open bug bounty program, etc (ACM, N.D) (ACM, 2018).
    - Principle 2.5 and 3.7 of the ACM Code by consulting with independent researcher and taking prompt action(s) to know the scope and mitigate the

identified risks and vulnerabilities of their system (ACM, N.D) (ACM, 2018).

Moreover, the comparison between The ACM Code of Ethics and the British Computer Society (BCS) Code of Conduct, shows that:

- They both promote equal accessibility of IT benefits to society and human well-being, and competence (Wheeler, 2003).
- The ACM Code of Ethics is global while the British Computer Society (BCS) Code of Conduct is specific to UK (MSc-IT Study Material, 2010)

(ACM Code 2018 Task Force, 2018), (Trustee Board, 2022),

Lastly, I would like to thank my peers, Laura, Hamad and Mahamad for reviewing my post. They raised good points and concerns, like on open bug bounty programs been beneficial to improve security aspects of a system, however, challenges like, unaudited or untrusted 3rd parties can create security loopholes like data breaches, reverse engineering, etc (Malladi & Subramanian, 2020).

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].

Malladi, S. S. & Subramanian, H. C., 2020. Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations. *IEEE Software,* 37(1), pp. 31-39.

MSc-IT Study Material, 2010. *BCS Codes of Conduct and Practice.* [Online]
Available at: https://www.cs.uct.ac.za/mit_notes/ethics/htmls/ch04s04.html
[Accessed 02 July 2023].

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].

Wheeler, S., 2003. *Comparing Three IS Codes of Ethics - ACM, ACS and BCS.* South Australia, AIS Electronic Library .