**Laura: 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?**As a basic security mechanism, Corazón’s implant could only be accessible through short-range wireless connections, requiring the phone and implant to be in close proximity. Data transferred between the app and the device employed standard cryptographic algorithms, and all data stored locally on the phone was encrypted. To support on-going improvement, Corazón had an open bug bounty program inviting disclosure of potential vulnerabilities in their app.

At a recent security conference, an independent researcher claims to have found a vulnerability in the wireless connectivity

**Hamad: 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.** Data transferred between the app and the device employed standard cryptographic algorithms, and all data stored locally on the phone was encrypted. To support on-going improvement, Corazón had an open bug bounty program inviting disclosure of potential vulnerabilities in their app.

**Mahamad: 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.**

**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).**

The ACM Case study describes Corazón, a medical technology startup that develops an implantable heart health monitoring device. Let's review the application of the ACM Code of Ethics to this case study and highlight its impact on relevant legal, social, and professional issues, while also providing comparisons to the British Computer Society (BCS) Code of Conduct.

Impact on Legal Issues:

Corazón's compliance with multiple countries' medical device regulation agencies demonstrates their commitment to legal requirements and aligns with Principle 2.3 of the ACM Code, which emphasizes adherence to relevant laws and regulations.

The open bug bounty program implemented by Corazón encourages responsible disclosure of vulnerabilities. This approach can help identify and address potential legal issues related to data security and privacy breaches.

Comparison to BCS Code of Conduct:

The BCS Code of Conduct emphasizes compliance with legal obligations (Principle 1) and promoting the public interest (Principle 2), similar to the ACM Code. Both codes recognize the importance of complying with legal frameworks.

Impact on Social Issues:

Corazón's commitment to providing free or reduced access to patients living below the poverty line demonstrates their effort to address social inequality and improve healthcare accessibility (Principle 1.1 of the ACM Code).

By integrating technology into healthcare infrastructure, Corazón contributes to societal well-being and human welfare, as outlined in Principle 3.7 of the ACM Code. The collaboration with charities further exemplifies this commitment.

Comparison to BCS Code of Conduct:

The BCS Code emphasizes social responsibility (Principle 3) and aims to use technology for the benefit of society. Corazón's efforts align with these principles, as they prioritize social impact through their charity collaborations and heart health monitoring device.

Impact on Professionalism:

Corazón's adherence to robust security practices, such as employing standard cryptographic algorithms and inviting vulnerability disclosure, reflects professionalism and commitment to user safety (Principle 2.9 of the ACM Code).

Corazón's consultation with an independent researcher and their prompt action to mitigate the identified vulnerability highlight their commitment to comprehensive risk analysis and responsible behavior (Principle 2.5 of the ACM Code).

Comparison to BCS Code of Conduct:

The BCS Code emphasizes professional competence (Principle 1) and integrity (Principle 2). Corazón's use of standard cryptographic algorithms, vulnerability disclosure program, and consultation with external experts align with these principles, demonstrating professionalism and ethical conduct.

In summary, the application of the ACM Code of Ethics to the Corazón case study showcases their adherence to principles related to societal well-being, legal compliance, security, professionalism, and risk analysis. Corazón's commitment to providing affordable access, collaborating with charities, and promptly addressing vulnerabilities demonstrates their ethical approach to technology development and deployment. The comparison to the BCS Code of Conduct reveals similar ethical principles guiding the actions of computing professionals involved in this case study.