**ACM Ethics**
*The Official Site of the Association for Computing Machinery's Committee on Professional Ethics*

## Case: Medical Implant Risk Analysis

### Using the Code: Medical Implant Risk Analysis

Corazón is a medical technology startup that builds an implantable heart health monitoring device. The device comes with a smart phone app that can monitor and control the device wirelessly, as well as storing a persistent record that can be shared with medical providers. After being approved by multiple countries' medical device regulation agencies, Corazón quickly gained market share based on the ease of use of the app and the company's vocal commitment to securing patients' information. To further expand their impact, Corazón worked with several charities to provide free or reduced access to patients living below the poverty line.

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. The researcher presents a proof-of-concept demonstration where a second device in close proximity could modify commands sent to the implant to force a device reset. The attack relied on the use of a hard-coded initialization value stored in the implant device that created a predictable pattern in the data exchanges that could be manipulated. In consultation with Corazón's technical leaders, the researcher concludes that the risk of harm with this attack is negligible, given the limited capabilities of the device.

Analysis

Corazón's practices embody the goals of several principles in the Code. Corazón's products and their charity work contribute to society and to human well-being, consistent with the aims of Principle 1.1. By working within the regulations of governmental agencies, Corazón demonstrated a commitment to Principle 2.3. Corazón's use of cryptography and vulnerability disclosure adheres to the robust security goals of Principle 2.9. Furthermore, Corazón's reliance on standard cryptographic algorithms—rather than attempting to devise an unproven proprietary technique—shows commitment to Principle 2.6, restricting their developers' work to areas of competence.

Corazón's consultation with the researcher also highlights a key aspect of Principle 2.5. The design and implementation of Corazón's products exhibit a commitment to comprehensive and thorough risk analysis. Furthermore, Corazón welcomed independent security evaluation to identify additional issues that their designers overlooked. Once a potential vulnerability was discovered, Corazón acted responsibly and quickly to determine the scope of the flaw with the aim of mitigating the harm.

One area of concern regarding Corazón's design is the use of a hard-coded value in the implant. Given the nature of the device, fixing this design choice would be difficult if it proved necessary. However, there is insufficient evidence at this point to determine the scope of the risk induced by this design.

Corazón's on-going commitment to security and improvement also exemplify an important aspect of Principle 3.7. Corazón's rapid success in this specialized healthcare field is an instance of the integration of technology into the infrastructure of society. Recognizing the increased stewardship required by this Principle, Corazón began working with charities to serve individuals whose poverty may have excluded them from access.

*These cases studies are designed for educational purposes to illustrate how to apply the Code to analyze complex situations. All names, businesses, places, events, and incidents are fictitious and are not intended to refer to actual entities.*

---