The usage of “smart” implantable devices in medical settings is just beginning. Such devices include embedded chips in pacemakers or even automated syringe pumps for drugs/insulin. Society has had a general tendency to trust the medical community, as the mantra of all medical schools include the phrase, “primum non nocere” or “first, do no harm”; however, with the advent of modern technology, especially with the IoT and automated devices, the concept of “no harm” is no longer solely attributed to medical professionals. The medical field is reliant upon vast quantities of data in saving patients’ lives and to be able to treat them in a timely manner; the field, therefore, is in need of technologies that can automate some of the collection and processing of that data.

This need and incorporation of newer technologies by medical offices, hospitals, and networks have come across quite a few problems as vulnerabilities have arisen in the products that were being used. One of the more famous scenarios includes the recent fiasco of the more than 450,000 St. Jude Children’s Hospital’s pacemakers that were recalled in 2017 due to gaping vulnerabilities. The principle of doing no harm now lies amongst the companies that push out medical devices as well as the doctors providing the treatment through these devices.

Assets

- Human life
    - The goal of medicine is to save a human life and this is important as there exists potential behind every human life, with every person being able to contribute to a productive society. Therefore, these medical device companies also should have a responsibility and goal to protect the humans with the devices that they design and create.
- Patient Information
    - Patient information can be a treasure trove to malicious actors as it gives them avenues to blackmail patients with certain disorders/diseases, especially so with persons of prestige. The protection of patient information is vital to a functioning society as it not only helps with the decrease of stigma, but also the increase of care seeking behaviors in members of society, which is especially important with disease epidemics.

Threats

- Blackmail
    - As mentioned before, blackmail could be one of the biggest ways for adversaries to exploit vulnerabilities involving patient information. An example could be if a CEO of a mega corporation were to fall ill terminally, the company were to try to be surreptitious until certain matters were taken care of, and the news were to leak, then it could set off some sort of financial hiccup/chaos internationally (which could also be exploited). In this case, some sort of monetary blackmail or of the like could be pursued by these actors.
- General/Targeted Murder

    - If the vulnerabilities were critical, and it affected millions of people, malicious actors could threaten to wipe out those populations or subpopulations for whatever reason they may have. Malicious actors could also target murder people of power, maybe for instance the president or other world leaders for political/economic/etc. purposes.

Weaknesses

- Networked
    - By design, these medical devices are networked, and it introduces a whole host of vulnerabilities that are related to network security that the patient then has to worry about, such as being connected to the wifi at home. Another weakness in the design of these medical devices is that, if for instance any firmware update had to occur in person, then it introduces the costly and invasive procedure the patient has to incur.
- High Risk Updating
    - Should there be any critical bugs that impact the devices in a terrible way, such as the update bricking the device or draining the battery very quickly etc., then the patients have a lot more to worry about than the security of their devices. Once again, the fiscal costs could be high to the patient from constantly replacing the battery, as well as the risk of something going wrong and negatively impacting the patient.

Defenses

- Really the only defense is the way that the companies approach the product and security design as well as the implementation of the designs created. Hyper vigilance in understanding that the product the companies are dishing out affect human lives and creating the product and security design centered around that is the most important asset that these companies can have when creating something that affects a human life.

The risks are enormous when dealing with implantable medical technologies. As outlined above, an easily dark scenario can occur with the threat of murder at the forefront for not only certain individuals, but also anyone affected by a vulnerable device. Even indirect financial chaos can occur from the vulnerabilities that medical devices could have from either ransoms or the mining of patient information from these devices. There is a lot to lose and not too much to gain from the advent of these newer implantable medical devices with gaping vulnerabilities these days. As society is more aware of security through the media, there will most surely be pushback against companies that don't have security in mind when designing devices, such as St. Jude's. However there is room to improve and evolve, as mentioned before in designing a defensive system. It is true that nothing can be totally secure, however by making it ultra costly to these malicious actors through the well/securely designed and thoughtfully implemented devices, then these devices could possibly be a step towards revolutionizing medicine and the future. The developers of these technologies should have the same ethical motive as doctors, or even more so as technology becomes as important or even more so than the doctors who use them.

Sources

https://news.aamc.org/patient-care/article/exposing-vulnerabilities-how-hackers-could-target/

https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm

https://www.cybermdx.com/vulnerability-research-disclosures/alaris-tiva-syringe-pump

https://www.zdnet.com/article/fda-forces-st-jude-pacemaker-recall-to-patch-security-vulnerabilities/

https://www.medicalplasticsnews.com/mpn-north-america/cyber-vulnerabilities-found-in-two-major-medical-devices/

https://www.health.harvard.edu/blog/first-do-no-harm-201510138421

https://www.chartercollege.edu/news-hub/why-patient-confidentiality-so-important