Thank you Zihaad for your post explaining and identifying security threats and vulnerabilities that led to compromise the iStan mannequin. Accordingly, to Yaqoob and Atiquzzaman (2019) vulnerabilities and threats in medical devices such as the iStan mannequin are strongly related to communication protocols, design flaws in software and inappropriate security measures added during development.

For example, Man in the Middle (MITM) is an attack that occurs when someone intercepts the communication between a transmitting and a receiving node. The attacker deceives node 1 and node 2 by making them believe that communication is flowing in a secure channel, but attacker can intercept and modify the information flowing through it (Conti et al. 2016). Bluetooth Low Energy (BLE) a protocol alternative to Bluetooth is used by a wide variety of medical devices. It offers low power consumption and short latency periods, ideally for devices where battery life is important and sensed data accuracy is critical. Because of lack of robust authentication mechanisms, devices using BLE are susceptible to MITM attacks (Yaqoob and Atiquzzaman). Classen et al. (2018) demonstrated that measured data, credentials and private information from wearable medical devices using BLE was intercepted by using a customized app and connecting to the devices.

Regulations and mitigation techniques have been enforced in order to prevent personal health information to be leaked. One of those regulation is HIPAA (Health Insurance Portability and Accountability Act) that protects personal health information by requiring suitable privacy-related controls (Annas, 2003). Because of the limited availability of resources in medical devices security mitigation techniques are challenging to incorporate. Some of them proposed are Isolation-Based architecture and Data Flow Integrity mechanisms. The first consists on isolating sensible security parts of the system in an unreachable module and the last on verifying unchanged states of memory using pointers (Yaqoob and Atiquzzaman).

Yaqoob, T., Atiquzzaman, M. 2019. Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices. Available from: [**https://0-ieeexplore-ieee-org.serlib0.essex.ac.uk/stamp/stamp.jsp?tp=&arnumber=8703068&tag=1**](https://0-ieeexplore-ieee-org.serlib0.essex.ac.uk/stamp/stamp.jsp?tp=&arnumber=8703068&tag=1) [Accessed 16 November 2021].

Conti, M., Dragoni, N. 2016. A Survey of Man In The Middle Attacks. Available from: [**https://0-ieeexplore-ieee-org.serlib0.essex.ac.uk/stamp/stamp.jsp?tp=&arnumber=7442758**](https://0-ieeexplore-ieee-org.serlib0.essex.ac.uk/stamp/stamp.jsp?tp=&arnumber=7442758) [Accessed 22 November 2021].

Classen, J., Wegemer, D., Patras, P., Spink, T., Hollick, M. 2018. Available from: [**https://0-dl-acm-org.serlib0.essex.ac.uk/doi/pdf/10.1145/3191737**](https://0-dl-acm-org.serlib0.essex.ac.uk/doi/pdf/10.1145/3191737) [Accessed 22 November 2021].

Annas, G. 2003. HIPAA Regulations — A New Era of Medical-Record Privacy? Available from: [**https://www.nejm.org/doi/pdf/10.1056/NEJMlim035027**](https://www.nejm.org/doi/pdf/10.1056/NEJMlim035027) [Accessed 22 November 2021].