Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) **Compromising a Medical Mannequin.** Healthcare Information Systems and Technology (Sighealth)

- What are the major threats and vulnerabilities discussed in the paper?
- How would you mitigate against these?

Major threats	Vulnerabilities
The Government Accountability Office report (2012) concludes that the FDA faces challenges in how to identify medical device failures from intentional or malicious activities and that current policy and procedures are inadequate given the real security threats that exist Policy and procedures Logging These tensions include a) the need to fail encryption versus the impact on functionality and energy consumption. Identification, monitoring and control The authors indicate that there is a lack of research focusing on vulnerabilities in reprogrammable control devices.	Fu and Blum (2013) also highlight the MAUDE database does not adequately capture security-based failures or malfunctions for medical devices. Devices can be breached Residual data Networks infiltrated Architecture Brute force Denial of service
Mitigation	
Physical components out of use, e.g. USB drives Zero trust architecture Intrusion detection and prevention systems Education and training Policy	Firewalls CAPTCHA and two-factor authentication Medical devices need to consider security in their developing

From reviewing the paper "Compromising a medical mannequin" (Glisson et al., 2015), we understand the severe nature of threats and vulnerabilities the healthcare profession faces in society.

From the outset, Glisson et al. (2015) identify that the FDA's current policies and procedures are inadequate to deal with security threats (United States Government Accountability Office, 2012). The impact is significant given the risk posed to practitioners and patients, resulting in fatalities in a worst-case scenario. Education and training are crucial if staff maintain operational security (Anderson, 2008) to resist social engineering attempts and prevent negligent actions that could compromise security policies. Anderson (2008) suggests that a practical approach of two-factor authentication for login and CAPTCHA could mitigate attacks by brute force, which were indicated as a threat method (Glisson et al., 2015).

The article highlights how the FDA MAUDE database fails to capture impaired availability or malware infections in the medical device operating systems (Fu & Blum, 2013). This is significant to maintain the integrity and availability of the CIA triad (Troncoso, 2019). A compromised system would interfere with the safe practice of healthcare and a potential breach of patient data. The article highlights the severe risk of a compromised network that devices, such as pacemakers, could gather patient data and modify the device's behaviour, resulting in complications such as cardiac arrest. The conduct or functionality of the device could be threatened by a denial of service attack (Glisson et al., 2015). To mitigate these potential vulnerabilities, the use of intrusion prevention systems (Lerace et al., 2005) would support detecting anomalies of traffic and defence towards denial of service, notably as databases such as FDA's MAUDE does not support this. However, the use of an IPS may cause performance issues of the operating system, high cost and can incur false positive alerts, which can increase the workload of administrators. However, the IPS would support mitigation, offering detection and logging capabilities to reduce device vulnerabilities such as in the icsma-20-343-01 case in GE imagery and ultrasound products (Cybersecurity and Infrastructure Security Agency, 2020).

Cybersecurity and Infrastructure Security Agency. (2020). ICS Medical Advisory (ICSMA-20-343-01). Available: https://us-cert.cisa.gov/ics/advisories/icsma-20-343-01 [Accessed 13 November 2021].

Fu, K. & Blum, J. (2013). Controlling for Cybersecurity Risks of Medical Device Software. *Communications of the ACM,* 56, (10): 35-37.

Glisson, W., Andel, T., Mcdonald, J., Jacobs, M., Campbell, M. & Mayr, J. (2015). Compromising a Medical Mannequin. Available: https://www.researchgate.net/publication/281487935_Compromising_a_Medical_Mannequin [Accessed 13 November 2021].

Lerace, N., Urrutia, C. & Bassett, R. (2005). Intrusion prevention systems. Available: https://doi.org/10.1145/1071916.1071927 [Accessed 13 November 2021].

Troncoso, C. (2019). Privacy & Online Rights Knowledge Area Issue 1. Available: https://www.cybok.org/media/downloads/Privacy__Online_Rights_issue_1.0_FNULPeI.pdf [Accessed 13 November 2021].

United States Government Accountability Office. (2012). Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices. Available: https://www.gao.gov/assets/gao-12-816.pdf [Accessed 13 November 2021].