Medical companies must prioritise security to maintain the CIA triad and alleviate potential risks to human life. In this summary, we evaluate the role technology and training play.

Glisson et al. (2015) identify that the FDA's current policies and procedures are inadequate to deal with security threats. Education and training are crucial for staff to maintain operational security (Anderson, 2008), resist social engineering attempts, and prevent negligent actions that could compromise security policies. Abdulhak (2021) explains employees need a deeper understanding of malware and the capabilities that could harm the system (Abdulhak, 2021). Anderson (2008) also suggests that a practical approach of two-factor authentication for login and CAPTCHA could mitigate attacks by brute force (Glisson et al., 2015). Abdulhak (2021) further supported suggesting a basic DDoS attack could occur through vulnerable logins (Fruhlinger, 2018). The use of honeypots (Al-Jameel & Alanazi, 2021) could be an effective mitigation tool as part of a policy to disrupt attackers attempts and gain logs of attack strategies to improve future medical device development. However, actions should not be the sole responsibility of companies. Patients should also consider their actions in the process and how their negligence could cause vulnerabilities. Reassurance is welcomed that many governments support the need to introduce a minimum digital living standard in the hope that all users support minimising threats (B.C.S., 2021).

FDA MAUDE database fails to capture malware (Fu & Blum, 2013), which significantly risks integrity and availability (Troncoso, 2019), hindering the safe practice and breach of patient data. Qasim (2021) highlighted how the medical community has witnessed a surge in reported vulnerabilities, and the sector is unprepared (Qasim, 2021). Devices such as pacemakers gathering patient data could modify the device's behaviour, resulting in disastrous consequences to human life. Mitigations including intrusion prevention systems (Lerace et al., 2005) would support detecting traffic anomalies and defence towards denial of service. IPS do offer 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). However, IPS may cause performance issues of the operating system, high cost, and administrators' workload. Healthcare privacy is governed by HIPAA (C.D.C., 2018) in the US; wearable or mobile health devices are not. The IoT (Internet of Things) may provide the most significant challenge. Companies can support with software patches, secure boots, encryption so that users can enjoy the benefits of the cost-effective IoT devices; however, companies must try to establish a culture of security where staff are trained to recognise vulnerabilities (Chacko & Hayajneh, 2018).

Abdulhak, H. (2021). Peer Response. Available: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=285074 [Accessed 27 November 2021].

Al-Jameel, S. & Alanazi, A. A. (2021). Honeypots Tools Study and Analysis. Available: http://paper.ijcsns.org/07_book/202101/20210121.pdf [Accessed 17 November 2021].

Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd ed. Indianapolis, USA., Wiley.

B.C.S. (2021). Call for minimum digital living standard. Available: https://www.bcs.org/articles-opinion-and-research/call-for-minimum-digital-living-standard-by-professional-body-for-it/?utm_campaign=BCS%20Membership&utm_medium=email&_hsmi=186799310&_hsenc=p2ANqtz-_w6Hu9PDw1YdqqW2gajtIUruMDeSYBk6CF4t-Ebr-ZzRuOATRgGSazzcfE1x9ZoPU4oYBR3GVrcpuisBqdTUVNs8wCeaJ7bSSQbbx5M75GZ4Oz274&utm_content=186799310&utm_source=hs_email [Accessed 27 November 2021].

C.D.C. (2018). Health Insurance Portability and Accountability Act of 1996 (HIPAA). Available: https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge. [Accessed 27 November 2021].

Chacko, A. & Hayajneh, T. (2018). Security and privacy issues with IoT in healthcare. *EAI Endorsed Transactions on Pervasive Health and Technology,* 4, (14).

Fruhlinger, J. (2018). The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet. Available: https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html [Accessed 27 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].

Qasim, M. (2021). Peer Response. Available: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=285074 [Accessed 27 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].