Thank you Zihaad for your valuable post, you mentioned here an important view to threats such as no logging or failure detection and transferring of data in plain text through the network. In addition, locking the devices in a secure place to keep them away from ant unauthorized persons is crucial.

Firch (2021) highlighted keeping operating systems and software up to date as software developers deploy patches to fix bugs or remediate the discovered vulnerabilities to maintain the security of software or system at all, moreover, changing default operating system policies for example default domain password policy such as enforce password history, maximum password age, minimum password length, password complexity requirement, and store password using encryption will improve the security and used as mitigation of threat and vulnerabilities of health devices.

The adoption of zero-trust architecture moves network security toward a model that allows restricted access to the application, network, and environment (Salvi, 2021). Keeping IT infrastructure secure by restricting access to only authorized persons can be the first door of defense against the unwanted intruder.

References

Firch, J. (2021) What Are The Common Types Of Network Vulnerabilities. Available from: https://purplesec.us/common-network-vulnerabilities/ [Accessed 22 November 2021].

Salvi, V. (2021) Cyber Vulnerability is Healthcare’s Modern Malaise - ET HealthWorld. Available from: https://health.economictimes.indiatimes.com/news/health-it/cyber-vulnerability-is-healthcares-modern-malaise/86009989 [Accessed 22 November 2021].