Medical mannequins are used across the globe by students to carry out medical procedures. However, they are now heavily dependent on technology and this creates risks and vulnerabilities. During trainings, the authors identified that the Muse software allows the operator to control the mannequin remotely. Muse software is a browser-based application and this poses a threat of eavesdropping since information passes through the public internet. Thus there is need for proper tools to secure data. A VPN would be a great tool as it provides a high level of encryption to control the mannequins remotely.

Another vulnerability to note is that the mannequin uses adobe flash player as its front-end platform. The flash player comes with a lot of security issues. According to Locklizard (N.D) the flash player allows attackers to exploit and use maliciously crafted Flash content to crash the Flash player, and potentially take control of the affected computer. Once a hacker gets access to the computer, he will then deny access to the authorized user and they can now take all the information available. To worsen the situation, Adobe has since announced that it will no longer be supporting flash players. Hence, this can be mitigated by using HTML5 which has more protection and is more secure than the flash player.

References

Locklizard, N.D, Adobe Flash Player Security Issues, Exploit & Vulnerabilities, SWF Flaws. Available from: https://www.locklizard.com/adobe-flash-security/