Telemedicine Security

Shawn Villaverde

January 31, 2019

Telemedicine Security

Improved access to technology devices has allowed innovative ideas to flourish in different sectors, and the increased popularity of telemedicine in the twenty-first century points to the advances made in different sectors on account of the development in different forms of technology. However, the success of such programs largely depends on consumer confidence in using the different platforms, particularly due to security risks of the cyberspace. For instance, although a health practitioner or facility may invest in state of the art security features, there is no guarantee that the clients using the said platforms would use devices as secure. Ultimately, such poses risk to the entire system since hackers could just as easily access the central database if they accessed the client’s device during connection to the central database therein. Ultimately, this would be to the detriment of the entire system, and could even adversely affect other people’s motivation to use and share information through the different telemedicine applications and platforms.

It would be important to configure the different systems well enough to guarantee that the information shared is confidential enough and gets to the intended audience. Among some of the most common concerns in the use of telemedicine has always been the possibility of inadvertently sharing information that one may have intended to keep private (Hall &McGraw, 2014). Appropriate security protocols that prevent sharing of private information providing the users with some level of control would provide the users with increased levels of control unavailable if such security measures were unavailable.

Ultimately, the type of connection to the central server would be one of the primary factors influencing the quality of security features on the different platforms. Consistent monitoring of the platform to determine the possibility of areas of vulnerability would ensure that such issues are detected early enough and the appropriate measures are taken to mitigate the problems as they arise (Watzlaf, Dealmeida, Zhou, &Hartman, 2015). Ultimately, there would be limited chances of any extensive damage to the digital system without prior knowledge of the tech management team in the different healthcare professional environments.

Reference

Hall, J. L., & McGraw, D. (2014). For telehealth to succeed, privacy and security risks must be identified and addressed. *Health Affairs*, *33*(2), 216-221.

Watzlaf, V. J., Dealmeida, D. R., Zhou, L., & Hartman, L. M. (2015). Protocol for a systematic review of telehealth privacy and security research to identify best practices. *International journal of telerehabilitation*, *7*(2), 15.-22.