Secure wireless network technology in the hospitals

Student’s Name

Institution

Date

**Secure wireless network technology in the hospitals**

Wireless technology has evolved over the years, from a simple unmanaged network to an organization managed systems a defined centralized monitored and controlled wireless network. Hospitals or any healthcare settings are installed with wireless local area network, which is well defined with coordinated APs. The coordinated AP offers healthcare settings with well defined monitored, configured, controlled and management features which allow organization-level wireless local area network (WLAN) installations. The HIPAA deals with the standard to privacy for individual healthcare information. It also ensures that healthcare information of patients is protected. The whole concept of HIPAA Compliance is to make sure that data records or confidential and private information of patients are kept and not exposed to any third party.

In review of whether the organization has complied with the HIPAA standards, the entity, and the kind of privacy rules and the system protection established by the hospital. First, the level of access established by the hospital will be validated or checked whether it is up to standard required. The level of access should be based on the seniority of employees and usability. Therefore, it would be important to review the kind of access the hospital has installed. The access to WLAN includes guest, patients, administration, management and support access. Certain contents and usability must be limited to certain level within the network. Guest would only use the guest section to access the internet within the facility within a specific and defined time. According to (Osterhage, 2016), the seniority access ensures that individuals are only accessed to specific information within their use to avoid violation of patients’ privacy and confidentiality of information. It ensures that due diligent has been conducted in the hospital to establish the need and protection mechanism for efficient arrangement or assigning of access to the system.

In many cases, the information leak in most healthcare settings occurs when outsiders are allowed to use devices belonging to the institution. It would be important to conduct due diligent to establish whether the hospital practice Bring Your Own Device (BYOD) policy and the way system support biomedical devices and BYOD at the same time keeping the WLAN secure (Watfa, 2012). The virtual Private Network is also an important element in data protection. The wireless policy would be reviewed whether it provides direction on how to manage and address security issues of the hospital. The policy should forbid the unauthorized APs that can violate security and unauthorized reconfiguration of the network or the alteration of the APs (Jayakody, Srinivasan, & Sharma, 2017). The policy should also be established to limit WLAN traffic and to allow operation in a certain channels to limit the risk. The overview of the system would also include conducting due diligent to check whether the hospital has offer VPN training to employees and its usability within the hospital setup. All employees should be educated to use VPN at their workstation to limit the risk of data getting exposed or access by any third party (Jayakody, Srinivasan, & Sharma, 2017). VPN ensures that network access is under protection and invisible to any potential attacker.

In conclusion, securing patients’ information is the responsibility of the management of all healthcare settings. Therefore, in review whether hospital or any healthcare settings has complied with HIPAA, the entity, policy and hardware used would be reviewed to ensure that appropriate measures are in place to address any type of vulnerability, which can occur. The policy and standard should be strict to avoid any authorized entry by all measures possible.

# References

Jayakody, D. N., Srinivasan, K., & Sharma, V. (2017). *5G Enabled Secure Wireless Networks.* Chicago: Pearson.

Osterhage, W. (2016). *Wireless Network Security: Second Edition.* New York: Pearson.

Watfa, M. K. (2012). *E-Healthcare Systems and Wireless Communications: Current and Future Challenges.* England : Oxford Publisher.