**Professionalism data privacy vulnerability document**

**30030434**

**Introduction:**

Medical chatbots are becoming increasingly popular as they allow patients to interact with healthcare providers in a more convenient and efficient manner using the internet and software that imitates a human.

However, with the increasing use of these chatbots, there is also a growing concern over the security vulnerabilities they may face. In this report, I will discuss the data privacy vulnerabilities that medical chatbots may face and explore the solutions for these vulnerabilities.

**Data Privacy Vulnerabilities:**

Medical chatbots may contain sensitive information about patients, such as their medical history and personal details. If this data is not encrypted or protected appropriately, it can be easily accessed by hackers. It could also be stored on a database or a server and if that was hacked then it would affect the users data as it would have been in a data breach.

The chatbot may also share patient data with third-party providers, and other companies (insurers or pharmaceutical companies especially) that want to harvest user data for advertising purposes. This will further affect user privacy.

**Conclusion:**

Medical chatbots are becoming increasingly popular in the healthcare industry, but they are also vulnerable to data privacy vulnerabilities which is one of the critical issues that a medical chatbot may face. To mitigate these risks, and to protect sensitive data, chatbots should use end-to-end encryption and secure transmission protocols such as HTTPS. Additionally, chatbots should not store any personal data or medical information locally on the device or server, as that may increase the risk of data breaches.By implementing these solutions and fixes, we can ensure that medical chatbots are secure and safe for patient use.

Source:

CIO. (n.d.). *Chatbot Security in the Age of AI*. [online] Available at: https://www.cio.com/article/419211/chatbot-security-in-the-age-of-ai.html [Accessed 27 Feb. 2023].