**Problem Analysis Statement**

1. **Introduction**

The adoption of Information Communication Technology in the smart healthcare system endangers patient's privacy due to hacking, malware, theft, misuse of information, and human error. Despite many healthcare experts claiming using ICT in a smart healthcare environment is beneficial and valuable, a wide range of research, patient testimonies, surveys, and studies have reportedly raised privacy concerns over the claims.

It is a significant concern that the majority of understanding on the use of information communication technologies in healthcare focuses on the advantages and positive outcomes it generates. Little is known and understood about the negative impact it creates. In many cases, smartphones, mobile apps, and wireless technology such as Airdrop, Wi-Fi, and Bluetooth are used in connected health to enable patients to communicate with their providers without regularly visiting them. With these information communication technologies, patients can send regular body readings to their doctors, helping them notice the problems and intervene faster. However, the privacy abuse that occurs along the process is never given the attention it deserves. For example, Healthcare practitioners post blogs on social media that include patient's private information without the patient's consent, scientists and technology experts use their information to conduct research and encourage science. Hackers take advantage of weak systems and steal patient's information for financial gains.

This reality has forced many American patients to deny medical care over the concerns that their private information would be put to the public. In addition to depression, anxiety, and trauma-related issues, privacy concerns have weakened people's confidence in the use of technology in healthcare, jeopardizing its ability to improve accessibility, efficiency, and effectiveness.

With many people supporting using ICT in smart healthcare due to its positive impacts, raising awareness over the negative impacts it brings will aid healthcare professionals, experts, and researchers in developing more effective healthcare information systems with patient's privacy in place and information at safety. Moreover, issues such as suicide, depression, anxiety, shaming, and other trauma-related issues that arise due to patient's records exposure will reduce.

1. **Proposed Solution**

According to multiple studies and research, the educational approach is the most reliable way to solve the problem. Educating healthcare professionals on data protection during storage, capture, and transmission, establishing policies to passwords compliance, and safe pairing protocols would eliminate concerns expressed above. Also, such a solution would incorporate different extensive standards and regulations that would be needed to ensure strong privacy for all patients. For instance, to avoid posting pictures or videos, individual hospital numbers, or notes of patients without their permission on the internet, to avoid providing any specifics about patients that could be used to classify them during social media blogs, and to ascertain that no patient-related information can be found from healthcare practitioner's social media profiles.

1. **Conclusion**

To summarize all, the purpose of this research is to shed light on how the use of ICTs in smart healthcare poses risks to patient's privacy in the United States. The arguments that support the claim will be backed by scientific facts, statistics, surveys, and studies conducted from 2000 to 2021. With the objective to show the roots of the problem, this research will discuss different factors that cause patient data breaches in smart healthcare. Even though patient's medical records' security plays an essential role in their privacy, we will only focus on privacy in this research. Moreover, from the analysis of more than 15 sources, including research publications, studies, and surveys, this research will provide solutions to how healthcare sectors can address the problem by improving in ways that are "privacy-respecting and privacy reinforcing."