**Research Strategy**: < I am pursuing research on smart healthcare privacy from the perspective of ICT. Since the topic is broad, I chose to research on how the use of information communication technologies in smart healthcare endangers patient’s privacy. There are a lot of sources that talk about this topic. However, not all are credible. So, I used Google Scholar and Objee search to find sources that were both scholarly and peer-reviewed. To get sources that are closely related to my topic I searched keywords like “ICT”, “smart healthcare”, and “smart healthcare and privacy”. I got many sources, but to narrow it down I used web sources, journal articles, and research publications that were released from 1990-2021.>

**Algarni, A. (2019). A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems. IEEE Access, 7, 101879–101894.**[**https://doi.org/10.1109/access.2019.2930962**](https://doi.org/10.1109/access.2019.2930962)

Taken from the Institute of Electrical and Electronics Engineers, research into the use of information communication technologies in a smart healthcare environment shows that patient’s privacy is at risk due to different reasons. Those include 40% authentication, 24% authorization, 19% access control, and 17% others. The author argues that medical practitioners should have a secure and reliable way to keep patient’s sensitive and private information to prevent attacks and breaches from unauthorized users.

I selected this source because it discusses the same issue I am researching on and it also provided me with information that defines my research problem. More specifically, this article provides me with surveys, graphs, and classifications of privacy research in the smart medical environment of ICT.

In addition to the source being reliable, it also contains information from other credible sources. Concerning the content, the author‘s arguments were not repetitive, the main points were presentable, and the graphs presented were understandable without further explanations. Furthermore, this article provided me with the information that will help me to explain to my audience the main goal of privacy in smart healthcare and the requirements when developing privacy using information communication technologies. Those requirements include all systems only used by authorized users, information to be maintained securely between communication parties and all patients’ private and sensitive information to be maintained at the highest security level.

**Azad, M. A., Arshad, J., Mahmoud, S., Salah, K., & Imran, M. (2019). A privacy‐preserving framework for smart context‐aware healthcare applications. Transactions on Emerging Telecommunications Technologies, e3634.**[**https://doi.org/10.1002/ett.3634**](https://doi.org/10.1002/ett.3634)

Information communication technologies are commonly used in hospitals to enhance the well-being, quality of life, and safety of people. Such devices produce data containing confidential patient information where improper access leads to consequences such as information exposure. In the paper, released by Transactions on Emerging Telecommunications Technologies, the authors argue that the patient’s information can be disclosed by both authorized users and unauthorized users. Based on the analysis of current policies for the protection of the privacy of patients, the authors suggested an improvement to the commonly used Salford model for the protection of privacy against attacks. This development will help to prevent information breaches whether from outsiders or people within the healthcare environment.

I selected this source because it provided me with information that supports my problem statement. specifically, this article provided me with the information that will help me to show the comparison between concerns about the unlawful release of information by medical practitioners and concerns about the systematic flows of information throughout the healthcare environment.

This source will also help the research audience to see that the authorized users can use communication technologies to intentionally release patient’s information to outsiders which is perceived as invading patient’s privacy. Furthermore, this source provided me with the scale of privacy threats to health information by organizations that keep patients’ medical records. The source is credible, and the main points presented in the paper are straightforward which will help me during the analysis phase.

**Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on the blockchain with novel privacy risk control. Journal of Medical Systems, 40(10), 1-8. DOI:**[**http://dx.doi.org/10.1007/s10916-016-0574-6**](http://dx.doi.org/10.1007/s10916-016-0574-6)

Nowadays patients share their data and statics on apps with their trainers. Taken from the Journal of medical systems, the study shows there are concerns regarding using technology outside the clinical settings. Out of 24 medical-related apps, the study shows that 19 of them shared user data with 55 organizations for business purposes. The study concluded that medical practitioners should educate their patients regarding privacy concerns.

I selected this source because it provided me with information that addresses my research problem. More specifically, this article provided me the statistics to which patients’ medical records are exposed. These statistics will help me to understand how information communication technologies used outside the clinic is a major concern to the patient’s privacy. With this being something that I do without knowing the consequences, this source was particularly useful in my research development because it showed me that there are a lot of people that do the same without knowing it is dangerous.

The source is reliable, and the authors’ main arguments are self-explanatory, however, the author failed to explain which factors were considered when choosing medical-related applications to study on which I believe was important because not all applications are a fraud. Also, I think the authors should have also talked about how people can use these apps and still maintain their privacy since these apps play important role in everyday life.

**Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Differential Privacy Techniques for Cyber-Physical Systems: A Survey. IEEE Communications Surveys & Tutorials, 1–1.**<https://doi.org/10.1109/comst.2019.2944748>

Taken from the Institute of Electrical and Electronics Engineers, a survey shows that online challenges to the privacy of patients are growing as healthcare institutions rely more on technology to communicate with patients. Statistics show that 79% of the technology used between doctor-patient communication is vulnerable to cyber-attacks which results in patient’s information being disclosed to unauthorized users. For example, nowadays, patients use heart-rate sensors, and temperature sensors to monitor their daily readings. However, this information does not directly be transmitted to the intended person without a third party’s involvement. With this being a biggest the biggest concern, this article provides more reliable implementations that will address patient’s privacy concerns.

I selected this source because it provided me with information that addresses my research problem. More specifically, this article will provide me with data regarding the surveys and statistics of which advancements in ICT have affected certain patient’s privacy. Moreover, this source helped me to learn more about the usefulness of the doctor-patient privacy relationship which is important in my research.

The source is credible, and the authors provided evidence that supports the arguments. However, the author did not propose solutions that can help to mitigate the risk which I think would have been important as well.

**Matthew. B (2016). Privacy risks when using mobile devices in health care. PubMed Central (PMC).**[**https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5008929/**](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5008929/)

In the article released by the US National Library of Medicine, Bromwich, a Head surgeon at children’s Hospital argues that mobile phones have changed the healthcare environment for the better. However, it has also brought substantial risk in terms of patient’s privacy. For example, in some circumstances where mobile devices are stolen or hacked, hackers widely share patient’s images and information on social networks without their consent. Not only does this affect patient’s privacy but also gives rise to civil liability and statutory. In addition to showing the privacy risks associated which using mobile devices in healthcare, the author also provided the standards in which patients’ privacy should be upheld and provided some guidance on what to do in the event of a breach.

I chose this source because it provided me with information that addresses my research problem. Specifically, it helped me see how mobile phones play a role in risking patient’s privacy. Furthermore, it will help the research audience in general to compare the role of different information communication technologies in risking patient’s privacy.

 this article is relatively straightforward, and the main points are presented with evidence that supports the arguments. Also, when I read another article that talks about the role of mobile phones in healthcare privacy, the central argument was the same.

**Rindfleisch, T. C. (1997). Privacy, information technology, and health care. Communications of the ACM, 40(8), 92–100.**[**https://doi.org/10.1145/257874.257896**](https://doi.org/10.1145/257874.257896)

In the article written by Thomas, a senior research scientist at Stanford University, a system view of information communication technology and patient information privacy is considered. Thomas outlines threats that certainly arise because of modern failed implementations of the use of information communication technologies in healthcare. Those risks include medical records in the hands of unauthorized users and medical practitioners failing to enter all information into patients' records in the fear of break-ins. Furthermore, He presented the main privacy policy problems that need to be resolved in the smart health care environment. Those include, too many people having access to patient’s records, failed to have authentication cards, and communicating using unprotected resources.

I selected this article because it will be useful to my research by providing me with the information that defines my research question. This source is credible, and the arguments presented by the author have evidence. The author’s arguments are not repetitive, and the information is understandable without more explanations. However, the article is outdated(1997) and the topic requires current information.

 This is useful to my research because I will use it to show that too many people have access to medical records which threatens the privacy of the patients. And it will also help me the research audience to understand why the patients’ privacy needs to be maintained.