

RESEARCH PROPOSAL

TITLE:(The impact of cybersecurity breaches on patient safety and privacy within UK health care sector.)

June Lillian Truepenny (2514423)

Programme: Certificate of Higher Education Skills
For The Workplace (Health and Social Care)

Module: Digital Skills and Research Methods

Module Code: LCHS4007

Lecturer: Hajra Mustasim (Module Lead)

Contents

1. INTRODUCTION	3
1.1 Research Aim and Objectives	3
1.2 Research Questions	3
1.3 Research Topic Identification.	4
2. JUSTIFICATION FOR RESEARCH.....	5
2.1 Information Sources.....	5
3. RESEARCH METHODOLOGIES	6
3.1 Overview of Research Methodologies.....	6
3.2 Data Collection.	6
4. CONCLUSION.....	8
REFERENCES	9

1. INTRODUCTION

This research will aims to analyse about the impact made by the cybersecurity breaches upon the patient safety as well as the privacy within the UK healthcare sector. As the healthcare organizations are very increasingly relied on the digital systems to store and process sensitive patient data, the risks which is been associated with the cybersecurity breaches have escalated. This study will help to examine the issues which are faced by the healthcare organizations, explore the strategies which is been applied to protect the patient privacy, and assess the consequences of all these breaches upon the safety of patient (Cartwright, 2023). The research will help to make the secondary and qualitative sources, by the help of case studies from UK healthcare sector to give an in-depth analysis of these issues.

1.1 Research Aim and Objectives

Aim

The research aims to analyse the impact of cybersecurity breaches on patient safety and privacy within UK health care sector.

Objectives

- To study the concept of cybersecurity breaches on patient safety and privacy within UK health care sector.
- To examine the challenges faced by the UK health care sector in maintaining the patient safety and privacy due to the absence of effective cybersecurity measures.
- To identify the strategies used by the UK health care sector to effectively maintain the patient privacy and ensure cybersecurity.
- To determine the impact of cybersecurity breaches on patient safety and privacy within UK health care sector.
- To provide meaningful recommendations to UK health care sector for improving cybersecurity measures to effectively protect the patient safety and privacy.

1.2 Research Questions

1. What is the concept of cybersecurity breaches on patient safety and privacy within UK health care sector?

2. What are the challenges faced by the UK health care sector in maintaining the patient safety and privacy due to the absence of effective cybersecurity measures?
3. What are the strategies used by the UK health care sector to effectively maintain the patient privacy and ensure cybersecurity?
4. What is the impact of cybersecurity breaches on patient safety and privacy within UK health care sector?

1.3 Research Topic Identification.

Current Issue in the UK Health and Social Care Sector

The cybersecurity breaches are a very rapidly growing issue within the healthcare sector, with the sensitive data of the patient at risk because of the vulnerabilities in the digital systems. All these kind of breaches can lead to loose the data, identity fraud, and, a more critically, the compromise of patient safety by doing the delays in treatment. The UK healthcare sector has also witnessed various high-profile cybersecurity breaches, which shows a need for an effective security measures (Tully et al., 2020). This research will keep its focus upon understanding about the scope and also the impact which is been created by these breaches, specifically upon the patient safety and privacy, within the healthcare system of UK.

Also the groups which have been affected are mainly the primary stakeholders within the healthcare are patients, healthcare providers, and even the organizations. The patients have to face the risk of having their personal and medical information getting leaked, this thing can lead to raise the issue of identity theft, financial fraud, and emotional distress (Nifakos et al., 2021). The healthcare providers are been impacted by the loss of patient trust and the potential legal and financial penalties. The organisation indulge within the healthcare will also face the problem in service delivery, reduced reputation, and also the costs of responding to effectively mitigate the breaches. All such breaches also have broader implications for the public confidence in the use of digital technologies within healthcare.

2. JUSTIFICATION FOR RESEARCH

As the healthcare systems are rapidly digitized, the cybersecurity breaches shows a significant risk to the confidentiality and also the safety about the data of patient data. The rising issue of the cyberattacks which will be targeting the institutions of healthcare, like the NHS, has highlighted the need for a comprehensive research upon the strategies, which will help to solve these risks (Triplett, 2024). By properly understanding these challenges, the current strategies, and also the impact made by the cybersecurity breaches is very critical, to enhance the UK healthcare sector's resilience to future threats.

2.1 Information Sources.

1. Source 1: "Cybersecurity in the UK Healthcare: Lessons from the past breaches"

This report helps to show the various kind of cybersecurity breaches within UK healthcare sector, which will be including those in the NHS, and gives an analysis of their impact made upon the privacy of a patient and their safety (Gupta, Kapoor and Debnath, 2025) . The source is relevant to get an understanding about the problems faced by the healthcare organizations in protecting the data of all the patients.

2. Source 2: "The Impact made by Cybersecurity Breaches upon the Healthcare Service Delivery"

This case study-based paper will help to evaluate that, how the cybersecurity breaches have make an impact upon the patient care, particularly in terms of delays, misdiagnosis, and the overall service quality (Salama, Altrjman and Al-Turjman, 2024) . Also it will help to give the insights, that how such kind of these breaches will affect the patient safety and how healthcare providers will respond to these mitigate the effects.

3. Source 3: "Securing the data of patient: Strategies as well as the Challenges within the UK Healthcare Sector"

By the help of this source, it will explore the strategies applied by the UK healthcare organizations, for protecting the patient data (Al Zaabi and Alhashmi, 2024). It includes examples of effective cybersecurity measures as well as the challenges, which is been faced by the organizations, to give valuable insights into the current landscape to improve the cybersecurity practices.

3. RESEARCH METHODOLOGIES

3.1 Overview of Research Methodologies.

- **Secondary Research:** The secondary research involves analysing the data, which has been already collected, like in the form of reports, case studies, academic articles, or the government publications (Gioia, 2021). In this study, by the help of secondary research, it will help to explore the existing case studies, reports, and the other literature upon the cybersecurity breaches done within UK healthcare sector. By this approach, it will also allow for the examination of a wide range of existing data.
- **Qualitative Research:** By the help of qualitative research, it will keep a focus on understanding the human experiences, their behaviours, as well as their perceptions. For this study, the qualitative research will involve the analysis of the case studies, which is basically from the UK healthcare organizations, who have experienced the cybersecurity breaches (Lochmiller, 2021). Also it will find out the strategies as well as the responses to these breaches from the perspective of the healthcare professionals, the policymakers, and the IT experts.

This research will make use of the secondary qualitative methodology. By using the secondary data, the research will analyse the existing case studies, articles, and reports which are related to the cybersecurity breaches within UK healthcare (Babii, 2020). With the help of Qualitative analysis the study will keep a focus on examining the impact made by these breaches, highlighting the experiences of the stakeholders who get affected, and also the understanding the strategies which are used to mitigate the risks. The qualitative approach will allow to get the in-depth exploration of human and organizational factors which are involved in the cybersecurity breaches.

3.2 Data Collection.

As the study will use the secondary data. It will include the existing case studies, reports, academic articles, and even the policy documents which are related to the cybersecurity breaches within UK healthcare sector (Djafar et al., 2021). This data will help to give insight into the scope of the issue, the strategies which are used by the healthcare organizations to address such kind of breaches, and their impact upon patient safety as well as their privacy.

Given the focus upon the case studies and existing literature, the secondary data will also help to collect the information about cybersecurity breaches done in the UK healthcare

institutions, the policies and measures in place to find out all these breaches, and the outcomes upon patient safety and privacy. Also the case studies will be properly analysed by doing the thematic analyses, to see that how these breaches rise, how they can effectively handle (Firdaus et al., 2021). As using of the use of secondary data will allow for comprehensive analysis about the real-world examples and it will also help in contextualize the study within the broader environment of UK healthcare.

4. CONCLUSION

This research aims to explore about the impact made by the cybersecurity breaches on the patient safety as well as their privacy within UK healthcare sector. By examining the case studies about the past breaches and also by analysing the secondary data, the study will effectively find the problems that the healthcare organizations have to face in properly maintaining the patient privacy and the effectiveness of their strategies to better and rapid mitigate the cybersecurity risks. Also the study will give recommendations to enhance the cybersecurity framework within UK healthcare system. The findings will be instrumental in improving the practices of patient data protection and also enhancing the resilience of healthcare institutions to the cyber threats. Ultimately, the research will help to give better insights to protect the patient safety in a rapid growing digital healthcare environment.

REFERENCES

- Al Zaabi, M. and Alhashmi, S.M. (2024). Big data security and privacy in healthcare: A systematic review and future research directions. *Information development*. doi:<https://doi.org/10.1177/02666669241247781>.
- Babii, A. (2020). Important aspects of the experimental research methodology. *Scientific journal of the Ternopil national technical university*, [online] 97(1), pp.77–87. doi:https://doi.org/10.33108/visnyk_tntu2020.01.077.
- Cartwright, A.J. (2023). The elephant in the room: cybersecurity in healthcare. *Journal of Clinical Monitoring and Computing*, [online] 37(5). doi:<https://doi.org/10.1007/s10877-023-01013-5>.
- Djafar, H., Yunus, R., DJ Pomalato, S.W. and Rasid, R. (2021). Qualitative and Quantitative Paradigm Constellation In Educational Research Methodology. *International Journal of Educational Research & Social Sciences*, 2(2), pp.339–345. doi:<https://doi.org/10.51601/ijersc.v2i2.70>.
- Firdaus, F., Zulfadilla, Z. and Caniago, F. (2021). Research Methodology : Types in the New Perspective. *MANAZHIM*, [online] 3(1), pp.1–16. doi:<https://doi.org/10.36088/manazhim.v3i1.903>.
- Gioia, D. (2021). A Systematic Methodology for Doing Qualitative Research. *The Journal of Applied Behavioral Science*, 57(1), pp.20–29. doi:<https://doi.org/10.1177/0021886320982715>.
- Gupta, S., Kapoor, M. and Debnath, S.K. (2025). Cybersecurity Risks and Threats in Healthcare. *Artificial Intelligence-Enabled Security for Healthcare Systems*, pp.39–64. doi:https://doi.org/10.1007/978-3-031-82810-2_3.
- Lochmiller, C. (2021). Conducting Thematic Analysis with Qualitative Data. *The Qualitative Report*, [online] 26(6), pp.2029–2044. doi:<https://doi.org/10.46743/2160-3715/2021.5008>.
- Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E. and Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, [online] 21(15), p.5119. doi:<https://doi.org/10.3390/s21155119>.
- Salama, R., Altrjman, C. and Al-Turjman, F. (2024). 8 - *Healthcare cybersecurity challenges: a look at current and future trends*. [online] ScienceDirect. Available at: <https://www.sciencedirect.com/science/article/pii/B9780443132681000030>.
- Triplett, W.J. (2024). Cybersecurity Vulnerabilities in Healthcare: A Threat to Patient Security. *Cybersecurity and Innovative Technology Journal*, 2(1), pp.15–25. doi:<https://doi.org/10.53889/citj.v2i1.333>.
- Tully, J., Selzer, J., Phillips, J.P., O'Connor, P. and Dameff, C. (2020). Healthcare Challenges in the Era of Cybersecurity. *Health Security*, 18(3), pp.228–231. doi:<https://doi.org/10.1089/hs.2019.0123>.