Northumbria University NEWCASTLE
Newcastle • London • Amsterdam

COURSEWORK COVER PAGE	
Module Code/Title:	LD4020 Foundation of Computing Technology
Module Tutor Name:	
Student Name (ID):	
Programme of Study:	BSc Computing [UG]
Coursework Title:	Individual Assignment
Word count:	

Submission Instructions:

1. Name your submission using the name convention, LD4020_<your tutor initial>_<your programme>_<your id><name>.docx, eg LD4020_BK_UG_w24012345John.docx is a submission for the student of BSc Computing attending Basel Khashab's seminar session.
2. Submit to Bb on or before 16:00, 20 May 2025

Declaration of that the submission is your own work

We confirm that:

☐ This assignment submission is our own, independent work.

☐ I have referenced the sources of information, ideas, and quotations that I have used in this submission and listed my sources in a bibliography.

☐ I have submitted the supporting documentation I have been asked for (e.g., notes, plans, etc - refer to your assessment brief).

Declaration of the Use of AI tool:

EITHER

☐ I have not used AI at any point in preparing this assignment.

OR

☐ I have used AI tools (including, but not limited to ChatGPT) to help me (select all that apply):

- ☐ Generate initial ideas in response to the question.
- ☐ Develop my structure.
- ☐ Generate ideas for examples / sources.
- ☐ Provide feedback and suggestions for improvement on my content.
- ☐ Edit and improve my spelling and grammar.
- ☐ Other**: please explain**: _____

☐ I have NOT used AI to generate whole sentences, paragraphs, sections, or the whole of this assignment and I understand that this would be considered academic misconduct.

Your signature:		**Date:**	

Table of Contents

Introduction

In a fast-evolving healthcare market, health practitioners worldwide must safeguard patient data. MediCare, a reputable local medical provider, is digitising. Switching from handwritten notes and paper appointment scheduling to EHRs and IoT for 24/7 health monitoring should improve results. MediCare may face data security and privacy issues due to digital transformation. Medical data is sensitive; thus, rigorous measures are needed to avoid data breaches, unauthorised invasions, and other privacy violations. It analyses real-world data privacy events to find patterns and concerns that affect MediCare. This study proposes a well-structured effort to teach all relevant stakeholders and create awareness about patient data protection in contemporary healthcare.

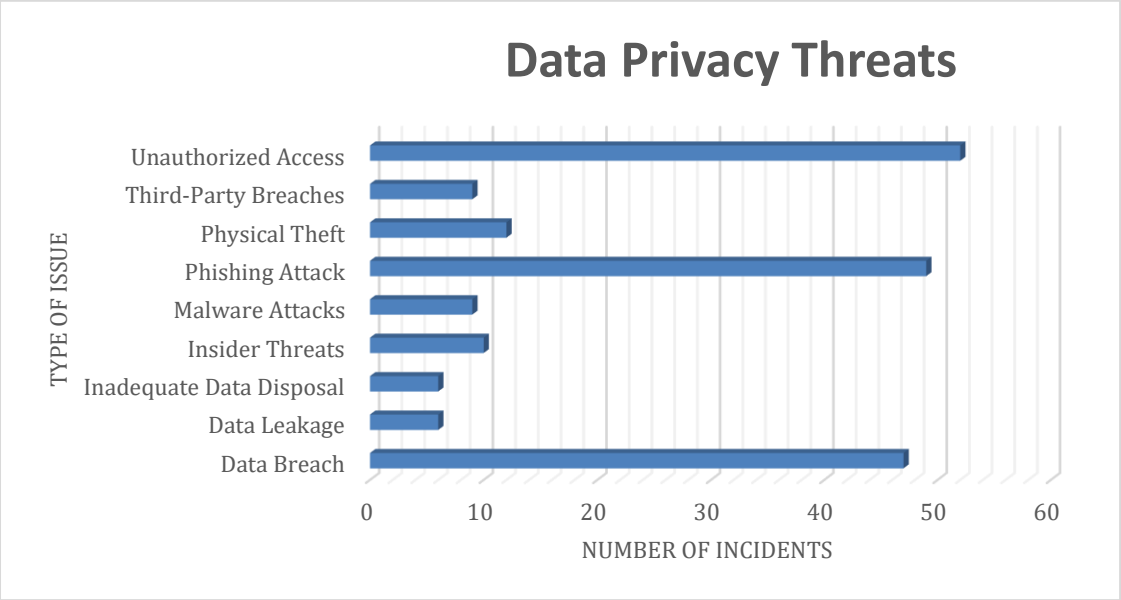
Task 1: Identifying Data Privacy Issues

Overview of the dataset

This report analyses MediCare data privacy events over the last year. A wide range of key metrics, including the type of data breach, the number of insider records involved, the date it occurred, the responsible entity, whether any regulations were broken, and the time taken to resolve each incident, are all tracked in detail. The nature and occurrence of data privacy violations within the organisation are clearly shown by these statistics. By utilising Microsoft Excel to analyse its dataset using multiple statistical approaches, MediCare learnt about its digital transformation problems in patient privacy. As a result, significant discoveries were made and the time- and category-based trends concerning incidents were clearly shown.

Data Privacy Threats at MediCare

A clear examination of the various privacy problems has shown that phishing attacks, unauthorised access and data breaches are often related to incidents.



The bar chart presents how often each type of threat occurs, allowing MediCare to identify areas where greater attention needs to be paid.

Most Common Types of Data Privacy Issues

Data analysis showed the relative occurrences of different categories of data privacy incidents suffered by MediCare during the last year, as summarised below:

Data Privacy Issues	Count of Type_of_Issue
Data Breach	47
Data Leakage	6
Inadequate Data Disposal	6
Insider Threats	10
Malware Attacks	9
Phishing Attack	49
Physical Theft	12

Third-Party Breaches	9
Unauthorized Access	52

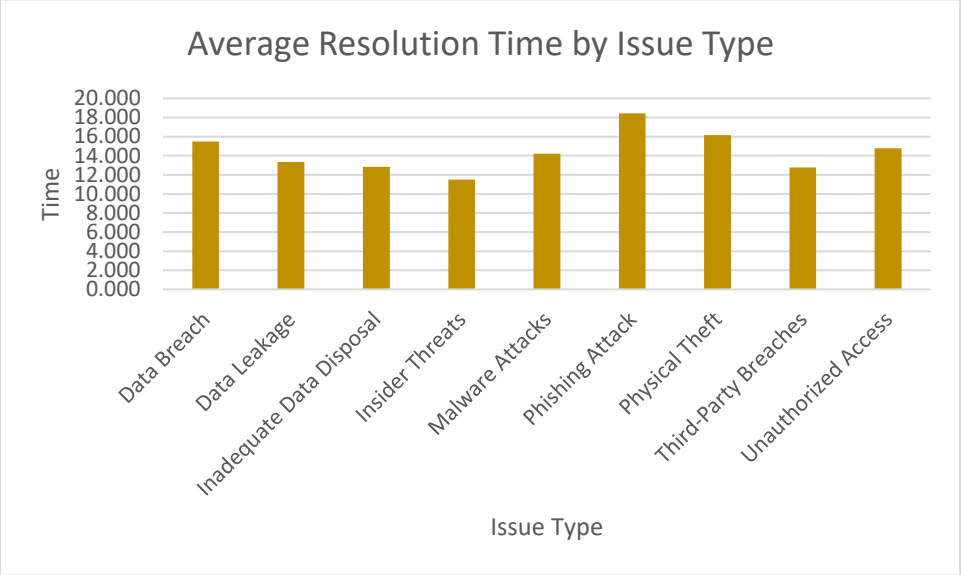
The data shows that unauthorised access and phishing attacks account for most instances. Unauthorised Access reveals system controls gaps, exposing patient data. Often caused by human mistakes, phishing assaults underscore the need for better staff cybersecurity training. Frequent data breaches indicate procedural and technical risks. Malware, insider threats, and physical theft are rare yet hazardous. Poor data disposal and leakage indicate data management and security problems. Maintaining consumer trust and complying with strict data protection regulations like the General Data Protection Regulation (GDPR) in Europe and the Payment Card Industry Data Security Standard (PCI DSS) globally requires protecting this data from cyber threats. Secure software development methods ensure that systems and applications are built with security in mind (Adesoga et al., 2024). This requires periodic vulnerability scans, code reviews, and security assessments to detect and repair issues before bad actors do. An effective financial cybersecurity strategy must include proactive threat identification and response. MediCare's data must be protected by strong cybersecurity and ongoing training throughout its digital transition.

Resolution Time by Type of Incident

The table below presents the average number of days it took MediCare staff to resolve each type of data privacy incident. These numbers show how long it takes to handle and fix each problem; longer times could raise the possibility of additional data exposure and damage to one's reputation.

Row Labels	Resolution_Time_Days
Data Breach	15.468
Data Leakage	13.333
Inadequate Data Disposal	12.833
Insider Threats	11.500
Malware Attacks	14.222
Phishing Attack	18.429
Physical Theft	16.167

Third-Party Breaches	12.778
Unauthorized Access	14.769



With longer resolution times comes a higher chance of more data breaches and worsening reputational harm to the company. To reduce the likelihood of such risks and maintain the confidence of stakeholders, it is essential to establish effective and coordinated incident response protocols.

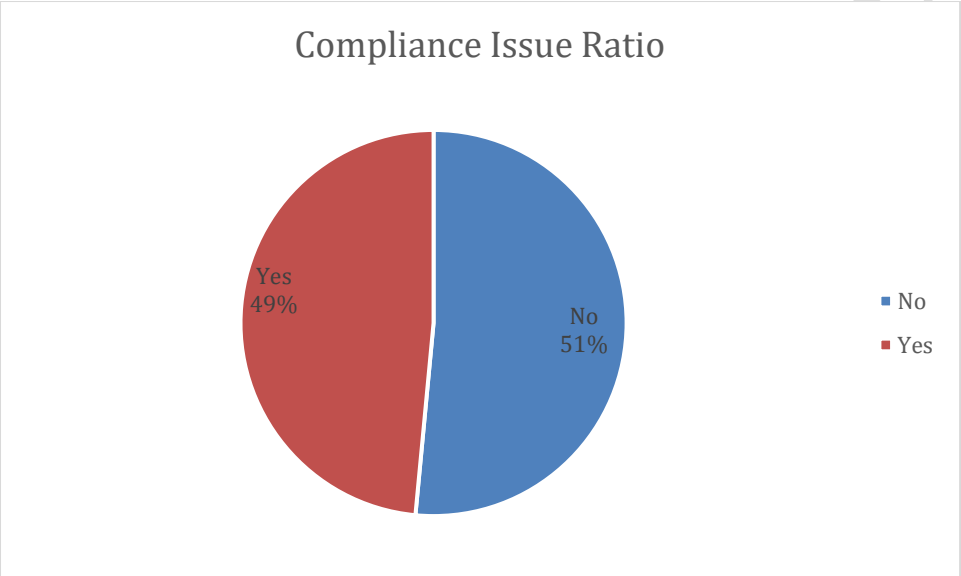
Source of Reported Incidents

Issues Reported By	**No**
External	64
Patient	64
Staff	72
Grand Total	**200**

The incidents were reported by 72 Staff reports, 64 patient reports, and 64 External Parties reports**.** This distribution implies that although staff reporting and internal understanding are generally high, outside sources are also quite important in raising awareness of data privacy concerns. The visibility and effect of these accidents beyond internal controls are highlighted by the significant number of reports from outside the company.

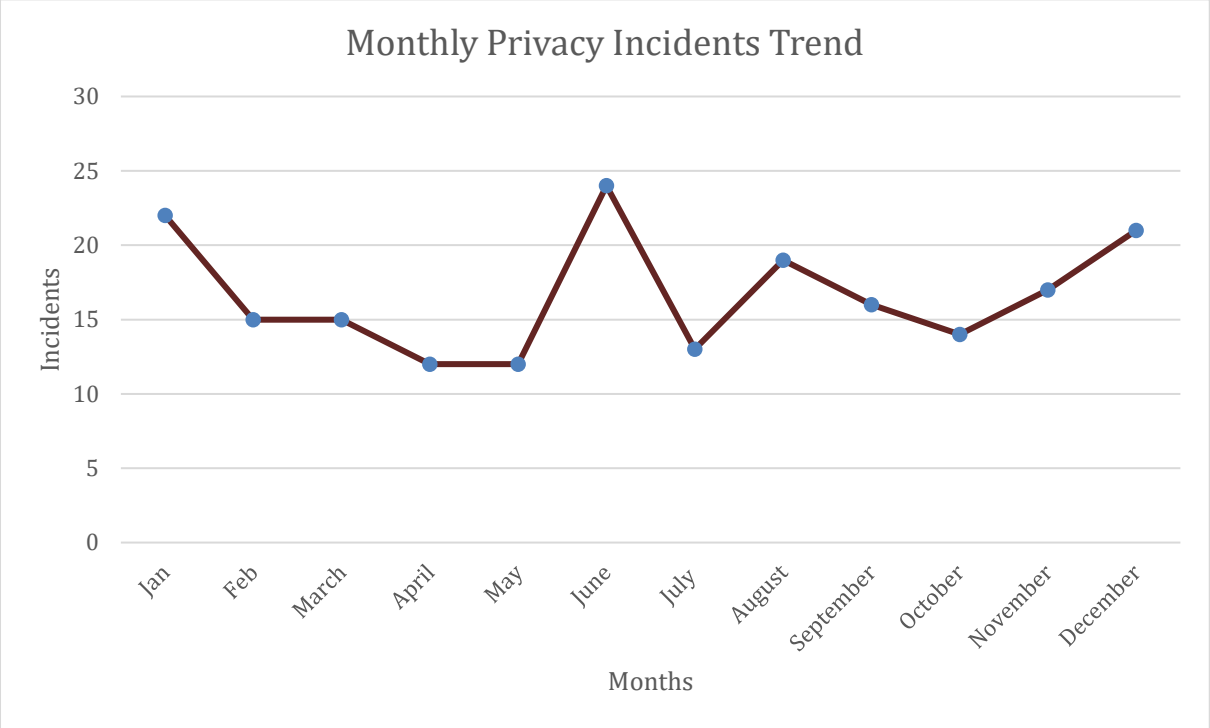
Compliance Issues

An examination of 200 reported incidents showed that 97 cases constituted 49% of the cases in which compliance guidance wasn't followed. However, 103 incidents, responsible for the other 51%, didn't involve any violations of compliance.



The fact that roughly half of all breaches did not follow the required ethical and legal data protection requirements is a major concern for MediCare. If the organisation is not compliant with legislation, it might face penalties and lose the trust of its patients.

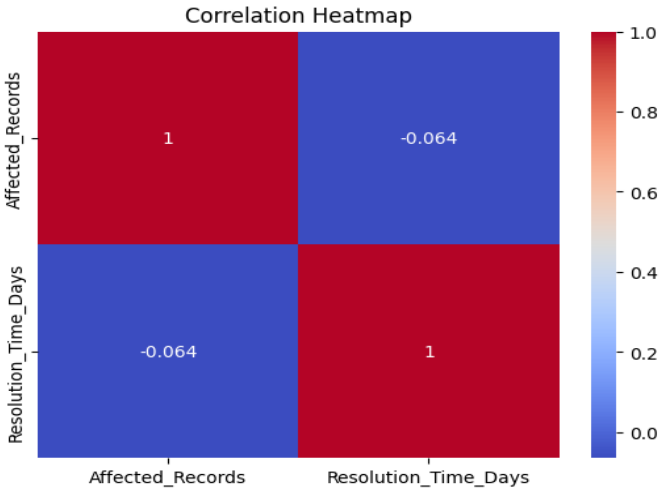
Monthly Trend of Incidents



These trends are the result of underlying causes that could lead to data security violations, such as staff changes, increases in workload, or system stressors at times.

Correlation Analysis

Resolution time and the number of impacted records had a weak negative relationship **(-0.064)**.



This suggests that longer incident resolution time frames do not always translate into more records being impacted. Inconsistencies in the management and resolution of various accidents

are shown by this poor association, which highlights the necessity for standardised processes to increase productivity and lower risks.

Task 2: Data Privacy Awareness Campaign Proposal

Campaign Objective

MediCare is launching a focused campaign called "Your Data, Our Duty" to limit privacy incidents and foster greater trust among staff and patients. This campaign intends to educate those within and outside the organisation on the most important aspects of safeguarding health data.

Campaign Goals

The campaign's main objectives are to raise patient, employee, and outside partner awareness of the dangers of data privacy.

- The primary goal of the campaign is to reassure patients that their information will be kept safe as they use MediCare's new digital system.
- To reduce the frequency of incidents caused by users, including data breaches or fraud resulting from cyberattacks.

This platform ensures compliance with laws and ethical practices while helping MediCare fulfil regulatory needs and strengthen its data security mindset (Pina et al., 2024). The campaign aims to build a sense of collective responsibility among healthcare professionals and MediCare staff to safeguard sensitive patient information by means of ongoing activities.

Target Audience

The campaign targets three key categories of people. Staff team, including doctors, nurses, administrators, and IT workers, must be trained in secure data handling to complete their work every day. Older patients who need property information about how their data is collected and protected are especially important for older and less technology-savvy individuals (Magsamen-Conrad et al., 2018). Partners and vendors who work with digital records are especially important since they process a wide variety of sensitive information and must adhere to strict data protection guidelines.

Key Activities

Staff Training Workshops: MediCare staff from every department will take part in these ongoing sessions, which will be held either in person or using Zoom. Attendees will learn important strategies for safeguarding sensitive data, including how to pick secure passwords, recognise fraudulent emails, and adhere to the confidentiality requirements of the healthcare industry (Ransdell et al., 2021). All MediCare employees will be expected to participate so that everyone understands and follows essential data privacy practices consistently.

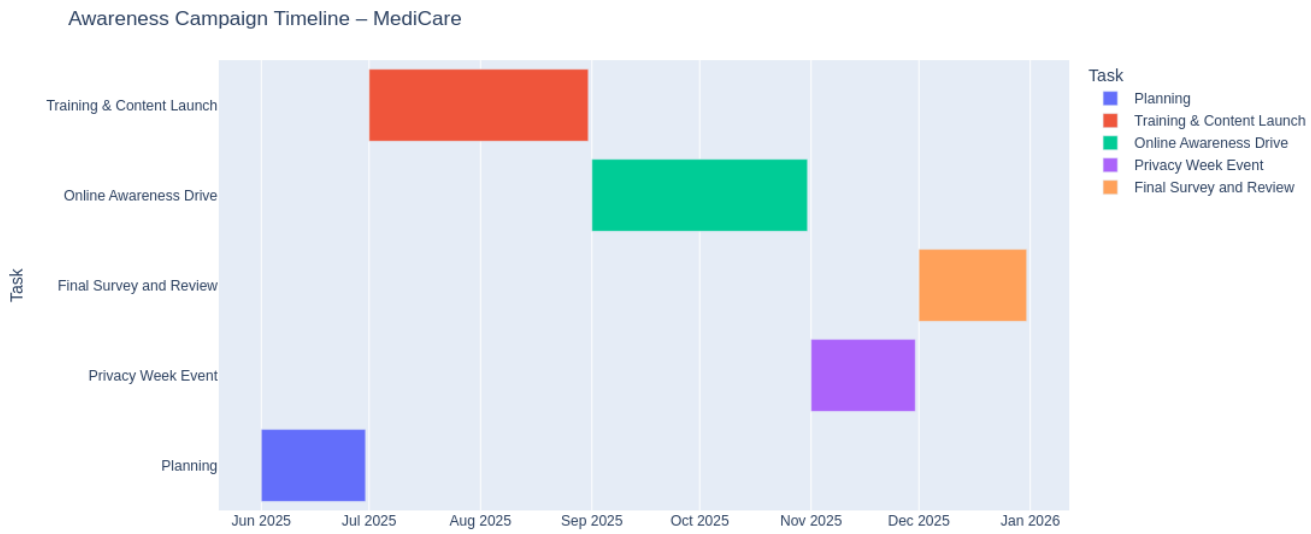
Patient Education Materials: Patients will find helpful pamphlets at convenient locations to learn more about the switch to electronic health records. Infographics included in these documents will outline the transition to EHRs and describe MediCare's approach to protecting patient information. Standard FAQs provide clear answers about how MediCare keeps patient information safe when it's exchanged or scheduled online.

Online Campaign: MediCare has unveiled a thorough online campaign to engage patients and the public in digital privacy and information security discussions. Various programs will educate and support safe cybersecurity methods. The program will include cyber safety education, a YouTube series on protecting private health data, and newsletters with frequent updates on internet security (Rahman et al., 2020). Developing a multi-front approach shows healthcare's greater focus on privacy and security (Khalid et al., 2023). Medicare must educate individuals on internet security so they may make educated choices, upholding data security and patient privacy.

Data Privacy Week Event: MediCare will host a one-week digital privacy awareness event each year with interactive activities. Expert guest speakers, interactive Q&A booths, and privacy-themed quizzes and activities will educate and delight attendees. The concept promotes active engagement and information exchange among staff and patients. MediCare will provide participants with gift vouchers to boost participation and learning. This campaign supports the organisation's effort to promote data protection and follows best practices in staff and patient cybersecurity education (Canadian Centre for Cyber Security, 2022).

Policy Update Communication: MediCare will share simplified data policies internally to raise awareness. In patient waiting rooms and staff lounges, big displays will convey policy points. This strategy promotes a transparent and informed organisation by providing clear and accessible data privacy information to workers and visitors.

Timeline



Phase	***Month***	***Activities***
Planning	June 2025	Content design, team setup
Training & Content Launch	July – Aug 2025	Staff workshops, materials distribution
Online Awareness Drive	Sept – Oct 2025	Social media + video content
Privacy Week Event	November 2025	Live engagement activities
Final Survey and Review	December 2025 – January 2026	Measure campaign impact

Roles and Responsibilities

- **IT Team:** This team is responsible for safeguarding the information infrastructure and helping develop the materials for information security training. They guarantee that the campaign's digital platforms are safe from security flaws.
- **HR Department:** Training session scheduling and attendance are managed by the Human Resources department. They are important in making sure that every employee takes part in privacy awareness training.
- **Marketing Team:** This group produces visual content, including flyers, posters, and social media posts. Their efforts aid in successfully conveying the campaign's message to patients and employees.
- **Compliance Officer:** The compliance officer monitors pertinent data privacy rules and regulations. They guarantee that the content of the campaign complies with the most recent legal requirements.
- **Physicians and Nurses:** Healthcare practitioners educate patients about data privacy best practices as privacy ambassadors. They encourage patient privacy, engagement and trust.

Metrics to Assess Impact on Patient Trust and Data Security Awareness

Medicare's campaign's effect on patient trust and data security awareness was measured using quantitative and qualitative measures. Participant trust levels increased after the campaign, demonstrating increased patient confidence in MediCare's data security measures (Flaubert, 2021). CTR and average instructional time were used to evaluate the campaign's digital outreach (Teo et al., 2024). Patient data privacy questions and support requests surged immediately following the campaign, suggesting patient awareness and proactive involvement. Patients understood and implemented security-recommended practices after the campaign, as two-factor authentication usage rose (Khalid and Akinlua, 2023).

The ad received generally positive feedback on social media, indicating that MediCare's data privacy commitment has improved (Russell, Rao-Graham and McNaughton, 2024). Internal privacy concerns decreased post-campaign, demonstrating enhanced patient openness and confidence. The Net Promoter Score (NPS) increased following the campaign, showing improved customer happiness and trust. Finally, throughout the campaign, privacy policy document views and downloads climbed dramatically, demonstrating greater data security knowledge and interest.

Metrics for Measuring Success

The Quantitative Metrics program seeks to significantly enhance data privacy procedures by reducing monthly reported occurrences by 50%. Furthermore, a 100% completion rate for staff training guarantees that every person is knowledgeable about security procedures. A 70% increase in accurate survey responses will be used to gauge patient participation, and 90% of new digital users should have faith in the system's security. In Qualitative Metrics, Staff and patient qualitative input, which offers insights into their perspectives and experiences, will also be used to gauge success (Hamilton and Finley, 2019). Evaluation of the campaign's overall effect on awareness will be aided by the degree of engagement on social media posts as well as the reach and clarity of informational materials.

Conclusion

The analytical evaluation and strategic solution to MediCare's data privacy issues are both skilfully covered in this report. Critical vulnerabilities that endanger patient information during digital transformation were identified by the investigation. These vulnerabilities include phishing, data breaches, and unauthorised access. A complete strategy is provided by the proposed "Your Data, Our Duty" campaign, which places a strong emphasis on communication, education, and clearly defined roles. MediCare can improve its technology infrastructure while protecting patient privacy and trust by putting this strategy into practice.

Reference list

Adesoga, T.O., Ojo, A.S., Olagunju, O. and Olaiya, O.P. (2024). Cybersecurity strategies in fintech: safeguarding financial data and assets. *GSC Advanced Research and Reviews*, 20(1).

Canadian Centre for Cyber Security (2022). *National Cyber Threat Assessment 2023-2024*. [online] Canadian Centre for Cyber Security. Available at: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024.

Flaubert, J. (2021). *The role of nurses in improving health care access and quality*. [online] *www.ncbi.nlm.nih.gov*. National Academies Press (US). Available at: https://www.ncbi.nlm.nih.gov/books/NBK573910/.

Hamilton, A.B. and Finley, E.P. (2019). Qualitative Methods in Implementation research: an Introduction. *Psychiatry Research*, 280(1). doi:https://doi.org/10.1016/j.psychres.2019.112516.

Khalid, N. and Akinlua, O. (2023). Enhancing Data Security in Healthcare Using Multi-Factor Authentication (MFA) Implementation. *ResearchGate*. doi:https://doi.org/10.13140/RG.2.2.14387.20001/1.

Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A. and Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Computers in Biology and Medicine*, 158(1). doi:https://doi.org/10.1016/j.compbiomed.2023.106848.

Magsamen-Conrad, K., Dillon, J.M., Billotte Verhoff, C. and Faulkner, S.L. (2018). Online Health-Information Seeking Among Older Populations: Family Influences and the Role of the Medical Professional. *Health Communication*, 34(8), pp.859–871. doi:https://doi.org/10.1080/10410236.2018.1439265.

Pina, E., Ramos, J., Jorge, H., Váz, P., Silva, J., Wanzeller, C., Abbasi, M. and Martins, P. (2024). Data Privacy and Ethical Considerations in Database Management. *Journal of Cybersecurity and Privacy*, 4(3), pp.494–517. doi:https://doi.org/10.3390/jcp4030024.

Rahman, N.A.A., Sairi, I.H., Zizi, N.A.M. and Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology*, 10(5), pp.378–382. doi:https://doi.org/10.18178/ijiet.2020.10.5.1393.

Ransdell, L.B., Greenberg, M.E., Isaki, E., Lee, A., Bettger, J.P., Hung, G., Gelatt, A., Lindstrom-Mette, A. and Cason, J. (2021). Best Practices for Building Interprofessional Telehealth: Report of a Conference. *International Journal of Telerehabilitation*, 13(2). doi:https://doi.org/10.5195/ijt.2021.6434.

Russell, S.N., Rao-Graham, L. and McNaughton, M. (2024). Mining social media data to inform public health policies: a sentiment analysis case study. *Revista Panamericana de Salud Pública*, 48. doi:https://doi.org/10.26633/rpsp.2024.79.

Teo, A.R., Rice, S.P.M., Meyer, E., Karras-Pilato, E., Strickland, S. and Dobscha, S.K. (2024). An approach to evaluation of digital data in public health campaigns. *Digital Health*, 10. doi:https://doi.org/10.1177/20552076241291682.