Research, Society and Development, v. 13, n. 6, e11313646080, 2024
(CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v13i6.46080

Investigating the intersections of vulnerability detection and Internet of Medical Things (IoMT) in healthcare, a scoping review protocol for Remote Patient Monitoring

Explorando as interseções da detecção de vulnerabilidades e IoMTs na saúde, um protocolo de revisão abrangente para Monitoramento Remoto de Pacientes

Investigando las intersecciones de la detección de vulnerabilidades y IoMTs en el cuidado de la salud, un protocolo de revisión exploratoria para el Monitoreo Remoto de Pacientes

Received: 06/03/2024 | Revised: 06/15/2024 | Accepted: 06/17/2024 | Published: 06/20/2024

Kulsoom S. Bughio
ORCID: https://orcid.org/0000-0003-4046-9578
Edith Cowan University, Australia
E-mail: k.bughio@ecu.edu.au
David M. Cook
ORCID: https://orcid.org/0000-0003-4046-9578
Edith Cowan University, Australia
E-mail: d.cook@ecu.edu.au
Afaq Shah
ORCID: https://orcid.org/0000-0003-2181-8445
Edith Cowan University, Australia
E-mail: afaq.shah@ecu.edu.au

Abstract

Due to the rapid and ubiquitous development and acceptance of IoT, healthcare providers have changed their locational settings from solely based in clinics to extend more broadly into the reach of patients' domestic homes. This IoMT focus extends to various medical devices and applications within the healthcare domain, such as any form of smartphones, surveillance cameras, wearable sensors, and actuators, that hold the capability to access IoT technologies. The aim of this scoping review has two important objectives. The first is to understand the best approaches towards acquisition and refinement of data in favour of an optimised cyber security posture for remote patient monitoring. The second is to understand how best to detect cyberattacks and vulnerabilities in Medical IoTs using automated reasoning. The review will be carried out according to the Joanna Briggs Institute (JBI) scoping review methodology. The key information sources are Springer Link, IEEE Xplore, Science Direct, SCOPUS, and ACM databases. The search is limited to studies written in English. The initial step in the review uses keywords and index terms to identify literature from the selected database information sources. The second step then takes the identified elements and searches each of the databases. The third step involves a search of the references to determine literature inclusion using a full-text screening process. Medical IoT devices, specifically designed for patient monitoring and diagnosis, excel in their ability to collect, transfer, and interact with real-time data. It focuses on intersections between IoMTs, cyberattacks and vulnerabilities, knowledge graph detection, and automated reasoning.

Keywords: Cyberattack; IoMT; Internet of medical things; Vulnerabilities; Knowledge graphs; Automated reasoning; Semantic modelling.

Resumo

Devido ao desenvolvimento rápido e ubíquo e aceitação da IoT, os provedores de saúde mudaram suas configurações de localização de base exclusivamente em clínicas para se estenderem mais amplamente ao alcance dos lares domésticos dos pacientes. Este foco em IoMT se estende a vários dispositivos médicos e aplicações dentro do domínio da saúde, como qualquer forma de smartphones, câmeras de vigilância, sensores vestíveis e atuadores, que possuem a capacidade de acessar tecnologias IoT. O objetivo desta revisão abrangente tem dois objetivos importantes. O primeiro é compreender as melhores abordagens para a aquisição e refinamento de dados em favor de uma postura de cibersegurança otimizada para o monitoramento remoto de pacientes. O segundo é entender como detectar melhor ataques cibernéticos e vulnerabilidades em IoMTs Médicas usando raciocínio automatizado. A revisão será realizada de acordo com a metodologia de revisão abrangente do Instituto Joanna Briggs (JBI). As principais fontes de informação são Springer Link, IEEE Xplore, Science Direct, SCOPUS e bancos de dados da ACM. A pesquisa é limitada a estudos escritos em inglês. O primeiro passo na revisão usa palavras-chave e termos de índice para identificar literatura das fontes de informação de banco de dados selecionadas. O segundo passo então leva os elementos identificados e busca em cada um dos bancos de dados. O terceiro passo envolve uma pesquisa nas referências para determinar a inclusão de literatura usando um processo de triagem de texto completo. Dispositivos IoMT médicos, especificamente projetados para monitoramento e diagnóstico de pacientes, se destacam em sua capacidade de coletar, transferir e interagir com dados em tempo real. Ele se concentra nas interseções entre IoMTs, ataques cibernéticos e vulnerabilidades, detecção de grafos de conhecimento e raciocínio automatizado.

Palavras-chave: Ciberataque; IoMT; Internet das coisas médicas; Vulnerabilidades; Grafos de conhecimento; Raciocínio automatizado; Modelagem semântica.

Resumen

Debido al rápido y ubicuo desarrollo y aceptación de la IoT, los proveedores de atención médica han cambiado su configuración de ubicación, pasando de estar basados únicamente en clínicas para extenderse más ampliamente hasta los hogares domésticos de los pacientes. Este enfoque en IoMT se extiende a varios dispositivos médicos y aplicaciones dentro del ámbito de la salud, como cualquier forma de teléfonos inteligentes, cámaras de vigilancia, sensores portátiles y actuadores, que tienen la capacidad de acceder a las tecnologías IoT. El objetivo de esta revisión exploratoria tiene dos objetivos importantes. El primero es comprender los mejores enfoques para la adquisición y refinamiento de datos a favor de una postura de ciberseguridad optimizada para el monitoreo remoto de pacientes. El segundo es entender cómo detectar mejor los ciberataques y vulnerabilidades en IoMT médicas utilizando el razonamiento automatizado. La revisión se llevará a cabo de acuerdo con la metodología de revisión exploratoria del Instituto Joanna Briggs (JBI). Las principales fuentes de información son Springer Link, IEEE Xplore, Science Direct, SCOPUS y las bases de datos de ACM. La búsqueda se limita a estudios escritos en inglés. El primer paso en la revisión utiliza palabras clave y términos de índice para identificar la literatura de las fuentes de información de la base de datos seleccionadas. El segundo paso toma los elementos identificados y busca en cada una de las bases de datos. El tercer paso implica una búsqueda en las referencias para determinar la inclusión de literatura utilizando un proceso de cribado de texto completo. Los dispositivos médicos IoMT, específicamente diseñados para el monitoreo y diagnóstico de pacientes, destacan por su capacidad para recopilar, transferir e interactuar con datos en tiempo real. Se enfoca en las intersecciones entre IoMT, ciberataques y vulnerabilidades, detección de grafos de conocimiento y razonamiento automatizado.

Palabras clave: Ciberataque; IoMT; Internet de las cosas médicas; Vulnerabilidades; Grafos de conocimiento; Razonamiento automatizado; Modelado semántico.

1. Introduction

The inclusion of scoping reviews as a process has gained significant approval and acceptance in recent times, whilst also drawing criticism and disapproval for the broad range of dissimilarities in the way some scoping reviews make choices regarding sources, inclusions, and extraction methods that can have a significant impact on the outcomes of a given scoping review (Pollock et al., 2022; Tricco et al., 2016; Peterson et al., 2017). While researching the background literature to seek intersections between vulnerability detection and IoMTs in healthcare, it became clear that the specific knowledge and information that directly informed the emerging knowledge vectors for this research area would depend upon a wide range of new and rapidly emerging knowledge. To ensure this knowledge was clearly understood and that clarity was based on both conceptual and technical reasoning, the literature review was re-defined to include a scoping literature review, with the expressed purpose of defining the new knowledge area, identifying gaps in knowledge, and identifying the emerging elements of greatest interest and application (Munn et al., 2018; Dean et al., 2019; Yii et al., 2020).

In the early stages of this study, a literature review was conducted to gather preliminary insights into the domain of the Internet of Medical Things (IoMTs), including telehealth, remote patient monitoring, and aged care. This initial stage further focused particularly on IoT medical devices used in remote patient monitoring, examining different techniques and methods used to identify vulnerabilities and cyberattacks in this application. These diverse domains served as a foundation for investigating various approaches, such as Explainable AI, blockchain, mining-based, and reasoning-based approaches.

To make these searches optimal and efficient, a scoping review became a useful mechanism to accurately determine the existing literature related to the interdisciplinary research area between IoMTs and cybersecurity. The scoping review is intended to map the breadth and depth of the available research, including key concepts, methodologies, and gaps in knowledge (Arksey and O'Malley, 2005). By conducting the scoping review, a researcher would be able to establish a comprehensive understanding of the field, identify research gaps, and determine the novelty and contribution of their work within this context.

The purpose of this scoping review is to summarize the existing evidence on the intersections between cyber security vulnerabilities, medical IoMTs, knowledge graphs, and automated reasoning within the last four years of publication. This review is designed to understand the key issues and gaps in this specific area of knowledge, and to understand what areas are emergent, evolving, dormant, or otherwise silent to the research audience. This approach provides the ability for the identification of ways to improve the protection of IoMTs from cyber-attacks, further provide clarity and intelligibility in terms of vulnerabilities, and improve levels of resilience to cyber-related malfeasance in the development of future medical IoT devices. The key outcomes for this review are twofold. The first is the explication of the existing knowledge on the intersections between cyber security vulnerabilities, medical IoMTs, knowledge graphs, and automated reasoning. The second is to originate a scope and understanding of the relevant issues pertaining to the resilience of IoMTs (MacNeill et al., 2022).

Principal Review Question

What has been found in relation to medical IoT devices within the inclusion of knowledge graphs, automated reasoning, cyber vulnerabilities, and cyber-attacks?

Sub Questions

How can data be optimized to support cybersecurity posture for the remote patient monitoring of IoMTs?
How can cyber-attacks and vulnerabilities can be detected by performing automated reasoning?

Inclusion Criteria

Table 1 shows the inclusion criteria for the study selection. It mainly includes the domain of research, the models and frameworks developed in this domain, and whether cyberattack and vulnerability detection are performed. The review includes papers that have been published in English and that appear in refereed journals, conference proceedings, and in published theses. Research that reviews IoMT frameworks, models or applications for remote monitoring systems are included in order to draw perspectives and known applications that inform the principal research agenda of the review. The review will include literature that demonstrates discourse with regard to cyberattacks or other vulnerabilities where they pertain to the internet of medical things (IoMTs) or areas of healthcare. The review also seeks to include discourse that debates the use of knowledge graphs that are used for the purpose of detecting vulnerabilities and cyber-attacks in in healthcare and/or IoMTs. In addition, the scoping review aims to include discourse that provides knowledge and information using the application of automated reasoning by rule-based practices. Research papers that are included must behold a general currency of less than 5 years since publication.

Table 1 - Inclusion criteria.

Inclusion Criteria	
No.	**Description**
1	The papers are in English from journals or conference proceedings or published theses.
2	Research presents a survey or review of the IoMT framework, models, or applications for remote monitoring systems.
3	Research inclusions discuss the cyberattacks and vulnerabilities within the Internet of Medical Things (IoMT) or healthcare.
4	Knowledge Graph for vulnerability/cyberattack detection specifically in healthcare/IoMT.
5	Articles are not older than the last five years, such as 2019-2024.
6	Studies discuss or demonstrate automated reasoning by rule-based techniques.

Source: Authors.

Exclusion Criteria

This scoping review protocol also maintains exclusion criteria for the literature, such as papers that are not in English or not peer reviewed. Only medical devices are considered, excluding other IoT devices like smartwatches or smartphones. Knowledge graph representation in non-medical domains is also excluded, as is the exclusion of automated reasoning that is not developed within a rule-based system, as described in Table 2.

Table 2 - Exclusion criteria.

Exclusion Criteria	
No.	**Description**
1	Not written in the English Language.
2	Not published in peer-reviewed journals or conferences.
3	Papers covering medical devices such as mobile phone sensors or smartwatches.
4	Papers for Knowledge Graph for vulnerability/cyberattack detection in other domains such as IoT networks.

Source: Authors.

2. Methodology

The review will be executed according to the JBI methodology for scoping reviews (Peter et al., 2020). The JBI methodology is an appropriate approach because it has received widespread usage, has been universally acknowledged, and provides clear steps on the supervision of scoping reviews. The scoping review method created by the Joanna Briggs Institute (JBI) is viewed as a robust method that provides strict guidance for researchers on the practice of conducting scoping reviews in healthcare and technology disciplines (Smith et al., 2022). This methodology describes adherence to the JBI approach on the basis that it includes strategies and information on developing review protocols, areas of study search and selection, and a clear method for data extraction and synthesis. A preliminary search of MEDLINE, the Cochrane Database of Systematic Reviews, JBI Evidence Synthesis, and CINAHL was conducted on the 14th of January 2024, and no current or underway systematic reviews or scoping reviews on this topic were identified or otherwise categorized.

Search Strategy and Database Inclusion

This approach draws from the three-point search strategy that is outlined in section 11.2.5 of the JBI scoping review guide (Peter et al., 2020). The first step of this strategy is to conduct an initial and limited search of the SCOPUS, SpringerLink, IEEE Xplore Digital Library, ACM Digital Library, and Science Direct using the following keywords: IoMT, rule-based reasoning, vulnerabilities, cyberattack, semantic modeling, and knowledge graph. The titles and abstracts of the relevant literature found will be analyzed, and the applicable index terms grouped and classified. The next step is to use all keywords and index terms to search the literature in each of the selected databases. The third step, screening reference lists, is then implemented for all studies that are selected for full screening (Campos et al., 2023).

Studies identified in this way are added to the title and abstract screening list and processed through stages 1 and 2 of the screening by two research assistants working independently from each other. An example of the search strategy for the SCOPUS database is included in the supplementary materials file included with this protocol. This strategy was developed with the assistance of an Academic Support Librarian (Baghbanian et al., 2020). The individual search terms and search string attributes can be significantly enhanced through a continuation of a collaboration with library-based search expertise in order to strategically improve a search strategy that ensures that relevant literature is found (Iannizzi et al., 2021). (See Table 3.)

To ensure the inclusion of high-quality research, this protocol places a reliance upon reputable sources such as SpringerLink, IEEE Xplore Digital Library, ACM Digital Library, SCOPUS and Science Direct. The protocol operates across five qualities within the search syntax. Each attribute forms an important policy structure to ensure the selection, order, structure and classification of key details which communicate the subsequent search string descriptors:

Table 3 - Search attribute policy.

Search Attribute Policy	
1	**TITLE-ABS-KEY**: This attribute entails searching for the selected keywords within the title, abstract, and keywords of the research papers/articles.
2	**AND**: This operator requires the presence of both keywords in the searched item i.e., IoMT and cyberattacks.
3	**OR**: This operator necessitates the presence of at least one of the terms in the searched item i.e., vulnerabilities or cyberattacks.
4	**NOT**: This operator excluded the terms and keywords from the literature.
5	**Year**: This attribute allowed us to specify the publication period range to align with the topic's timeline.

Source: Authors.

To refine the search for relevant articles and develop a specific results focus, this protocol follows a specific criterion (C) for each search string, which is intended to contain:

Table 4 - Search string criterion.

Search String Criterion	
1	**C1**: Semantic Modelling AND Knowledge Graph AND Vulnerability OR Cyberattack AND IoMT
2	**C2:** Automated Reasoning AND IoMT NOT Machine Learning NOT Deep Learning
3	**C3:** This operator Rule-based Reasoning AND cyberattacks OR vulnerability AND IoMT
4	**C4:** IoMT AND cyberattack OR Vulnerability AND knowledge graph.

Source: Authors.

The citations of all identified studies will be imported into a citation and reference management tool (for example Endnote or Mendeley) and all duplicate literature will be removed. The full citation list of theoretically appropriate studies is to be uploaded to the JBI System for the Unifies Management of the Assessment and Review of Information (SUMARI). (Aranas et al., 2023; Kirvin-Quamme et al., 2024; Mergen et al., 2023). Two research associates will then independently undertake stage one of the screening process through the application of the inclusion criteria. This takes place while an assessment of the titles and abstracts is undertaken to assemble and order potential studies.

Once stage one of this three stage process is completed only then can the second stage commence. In this case, the second stage takes place by means of the independent completion of full text screening for each study. It is important to note that the protocol described here is conducted using multiple independently operating research associates. These associates conduct screening independently of each other, and their screening decisions are recorded to show which papers are excluded, and by which of the research associates. Under normal conditions the minimum number of screening associates is two people, however this number can be increased to allow for a more accelerated number of independent assessments to take place. Under no circumstances should the full screening phase be completed by a single person, as this compromises the assurance of comparison and independent judgement and evaluation. This protocol works best with a team of three research associates but can include larger numbers in key phases where screening, evaluation and assessment decisions are discussed and fulfilled.

This process maintains a clear record of each screening and evaluation decision as a matter of record. Where conflicts arise from differences between research associates a final decision is reached after an inclusive session of discourse, and the final decision is made by an appointed researcher (Reid et al., 2019; Stewart et al., 2015). This process of transparency is maintained throughout the search and evaluation process and is kept in a recorded format which survives the entire scoping review progression. The results are also compiled and populated to show a visual representation of the competed process in the form of a Preferred Reporting Items for Systematic Reviews and Meta-analyses (PRISMA) flow diagram that is specifically designed for scoping reviews. (Page et al., 2021).

Data Extraction

A minimum of two researchers are required to use a data extraction tool to facilitate the extraction of relevant data from the included literature. A set of extraction details are recorded that show the publication year, the country, and the context of the technology inclusion (Cyber-attack, vulnerability, knowledge graphs, semantic modelling, and the association with IoMTs). The data extraction process is tested by two researchers independently extracting data from three studies. The results are then compared, and the extraction parameters revised to show areas of confluence. In each instance where an adjustment is made the change is recorded in the complete scoping review report. In instances where conflicts arise between researchers they are resolved by discussion. Where such discussion fails to resolve the conflict, the disputed position is referred to a single independent research associate for a final decision (Hall et al., 2021; Yanez et al., 2023).

Data Synthesis

The results from the extraction of data are populated into a table of results to provide a visual and openly inclusive means to establish, organise, and consolidate the surviving literature. The resulting data are united into a tabular document that sets out columns that differentiate each set of authors, publication years, countries, study designs, technology contexts and IoMT relationships. A narrative is composed at the conclusion of this table which expounds and develops the major themes and areas of data concentration that have emerged as a result of the extraction process applied to the literature.

3. Discussion

This review focusses on intersections between the increased identification and predictive power of a combinational approach that uses vulnerabilities, cyber-attacks, knowledge graphs, automated reasoning, and semantic modelling as a novel method of mitigation across incidents involving cybercrime involving medical outcomes concerning IoMTs. The confluence of these factors is anticipated to improve the identification and reduction of cyberattacks in transgressions that include the Internet of Medical Things (IoMTs) (John et al., 2022). It is a limitation of this study that there is a restriction to only consider sources of literature that are published in English. Future applications that use this protocol may benefit from a wider inclusion of IoMT sources that extend to literature written in languages other than English. As a specific benefit of this protocol the Joanna Briggs Institute follows a practice whereby it is not recommended to include a methodological appraisal that is based upon the quality of studies (Hercegovac et al., 2019; Peter et al., 2020). This may be regarded as a limitation in terms of preventing preferences to recommend some literature sources more strongly over others based on a system of quality-related ranking. It is, however, also a robust mechanism for the inclusion of sources where such pre-determined gradation ordering cannot be used to influence the outcome of a systematic review. A point of difference between scoping and systematic reviews is that scoping reviews are not required to measure and evaluate the quality of proofs, facts, and evidence, but rather to provide an outline and synopsis of the obtainable evidence rather than purely delivering synthesized findings or implementations (Lockwood et al., 2020; Iannizzi, 2021).

4. Conclusion

This scoping review methodology was employed to explore the standards, protocols, and recommendations to find out the approach for gathering adequate information to define a research area. The initial step involved sourcing relevant literature was executed using content analysis. Given that IoMT is an emerging technology, it is constantly changing and therefore requires frequent updates. Additionally, given the limited available research in the new and emerging areas of interest here, (and the relatively short timeline), the approach taken was to consider both peer-reviewed scientific publications, research articles and conference proceedings for examination. The single most critical need for many scoping review protocols is to provide a mechanism by which researchers can discover novel areas of pursuit in an area where fresh research is an imperative. Given that the specific knowledge area which bounds the focus of this scoping review protocol involves cyber security, it is often incumbent upon researchers to take new actions to recover emerging gaps and fresh research direction with which to battle against serious areas of human hardship (such as the ramifications of cyber-attacks and security-based hardships).

Scoping review protocols are important in terms of both guidance and direction. When followed prescriptively, they allow for a very high level of rigour that enables researchers to obtain a comprehensive overview of the specific literature relating to a given topic. More importantly, such protocols are instructive in terms of their ability to identify gaps in knowledge, and to address emergent changes in technology and knowledge application by indicating the most appropriate type of literature and study designs that are available. Such scoping reviews are of paramount importance under these conditions, where they contribute to the collation of knowledge that supports and enables research priorities to be set when used, controlled, and conveyed correctly. The aim of publishing this scoping review protocol is to provide a means of determining clear and appropriate rationale around cyberattacks and vulnerabilities aimed towards Medical IoT devices. The benefit of following a scoping review protocol, when undertaken in conjunction with the application of the JBI Handbook and the PRISMA-ScR visualisation process, is the expectation that research guidance becomes accurate, timely, and based upon both the available evidence, and a well-executed methodology.

To strengthen the knowledge value of this scoping review, it is essential to acknowledge its limitations. Firstly, this review exclusively focused on studies written in English due to the researchers' proficiency in the English language, potentially overlooking valuable insights from non-English studies. Although the review searched five comprehensive databases, likely, certain journals publishing English-language studies on vulnerability and cyberattack detection on medical devices may not have been included in the search. Consequently, while the review's scope is extensive, it cannot be deemed fully comprehensive.

It is worth noting that the study of vulnerability and cyberattack detection on medical devices is still in its early stages. Nonetheless, despite the relative immaturity of this research area, the inclusion of a substantial number of studies leads the researchers to believe that the results offer a valid summary of the available evidence. This scoping review fosters a comprehensive understanding of the issues in question, ultimately leading to more effective approaches for addressing vulnerability and cyberattack detection in medical device challenges in remote patient monitoring with digital technologies.

References

Aranas, L. L., Alam, K., Gyawali, P., & Mahumud, R. A. (2023). Examining Drug-resistant tuberculosis stigma among health care workers toward the development of a stigma-reduction intervention: Protocol for a Scoping Review. *JMIR Research Protocols*, 12(1), e43084.

Arksey, H., & O'malley, L. (2005). Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology*, 8(1), 19-32.

Baghbanian, A., Merlin, T., Carter, D., & Wang, S. (2020). Methods for the health technology assessment of complex interventions: a protocol for a scoping review. *BMJ open*, *10*(11), e039263.

Campos, L., Costa, D., Donato, H., Nunes, B., & Cruz, E. B. (2023). Implementation of digital health in rural populations with chronic musculoskeletal conditions: A scoping review protocol. *Plos one*, 18(12), e0291638.

Dean, J., Wray, A. J., Braun, L., Casello, J. M., McCallum, L., & Gower, S. (2019). Holding the keys to health? A scoping study of the population health impacts of automated vehicles. *BMC Public Health*, 19, 1-10.

Hall, P., Kroll, T., Hickey, J., Stokes, D., & Lennon, O. (2021). Patient and public involvement in stroke research: a scoping review protocol. *HRB open research*, 4.

Hercegovac, S., Kernot, J., & Stanley, M. (2019). How qualitative case study methodology informs occupational therapy practice: A scoping review. *OTJR: Occupation, Participation and Health (Thorofare N J),* 1539449219850123. https://doi.org/10.1177/1539449219850123

Iannizzi, C., Akl, E. A., Kahale, L. A., Dorando, E., Aminat, A. M., Barker, J. M., ... & Skoetz, N. (2021). Methods and guidance on conducting, reporting, publishing and appraising living systematic reviews: a scoping review protocol. *F1000Research*, 10.

John, B., McCreary, C., & Roberts, A. (2022). Smartphone technology for communications between clinicians–A scoping review. *Journal of Dentistry*, *122*, 104112.

Kirvin-Quamme, A., Kissinger, J., Quinlan, L., Montgomery, R., Chernenok, M., Pirner, M. C., ... & Robinson, A. (2024). Common practices for sociodemographic data reporting in digital mental health intervention research: a scoping review. BMJ open, 14(2), e078029.

Lockwood C, Tricco AC. (2020). Preparing scoping reviews for publication using methodological guides and reporting standards. *Nursing and Health Sciences* 2020;22 (1):1–4.

MacNeill, A. L., MacNeill, L., Doucet, S., & Luke, A. (2022). Professional representation of conversational agents for health care: a scoping review protocol. *JBI Evidence Synthesis*, 20(2), 666-673.

Mergen, M., Meyerheim, M., & Graf, N. (2023). Reviewing the current state of virtual reality integration in medical education–a scoping review protocol. *Systematic Reviews*, 12(1), 97.

Munn, Z., Peters, M. D., Stern, C., Tufanaru, C., McArthur, A., & Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC Medical Research Methodology*, 18, 1-7.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, *372*.

Peters, M. D., Godfrey, C., McInerney, P., Munn, Z., Tricco, A. C., & Khalil, H. (2020). Chapter 11: scoping reviews (2020). JBI manual for evidence synthesis. Retrieved January 2024, from https://jbi-global-wiki.refined.site/space/MANUAL/4687342/Chapter+11%3A+Scoping+reviews

Peterson, J., Pearce, P. F., Ferguson, L. A., & Langford, C. A. (2017). Understanding scoping reviews: Definition, purpose, and process. *Journal of the American Association of Nurse Practitioners,* 29(1), 12–16.

Pollock, D., Tricco, A. C., Peters, M. D., Mclnerney, P. A., Khalil, H., Godfrey, C. M., ... & Munn, Z. (2022). Methodological quality, guidance, and tools in scoping reviews: a scoping review protocol. *JBI evidence synthesis*, 20(4), 1098-1105.

Reid, A. E., Doucet, S., Luke, A., Azar, R., & Horsman, A. R. (2019). The impact of patient navigation: a scoping review protocol. *JBI Evidence Synthesis*, *17*(6), 1079-1085.

Smith, T., Lee, KH., Yu, K., Armstrong, L., **Cook, D.** M. **(**2022). Exploring issues of Resilience and Technology Use for Older People - A scoping review protocol. *Research, Society and Development*, 11(15), 1-6. https://doi.org/10.33448/rsd-v11i15.37773.

Stewart, L. A., Clarke, M., Rovers, M., Riley, R. D., Simmonds, M., Stewart, G., & Tierney, J. F. (2015). Preferred reporting items for a systematic review and meta-analysis of individual participant data: the PRISMA-IPD statement. *Jama*, 313(16), 1657-1665.

Tricco AC, Lillie E, Zarin W, O'Brien K, Colquhoun H, Kastner M, et al. (2016). A scoping review on the conduct and reporting of scoping reviews. *BMC Medical Research Methodology* 2016;16 (1):15.

Yanez, R. J. V., Fernandes, A. F. C., Mattos, S. M., Moreira, T. M. M., Castro, R. C. M. B., de Freitas Corpes, E., & Lopes-Júnior, L. C. (2023). Palliative care in the treatment of women with breast cancer: a scoping review protocol. *BMJ Open*, 13(6), e068236.

Yii, V., Palermo, C., & Kleve, S. (2020). Population-based interventions addressing food insecurity in Australia: A systematic scoping review. *Nutrition & Dietetics*, 77(1), 6-18.