Human Factors in Cybersecurity, Vol. 127, 2024, 225–235
https://doi.org/10.54941/ahfe1004782

Human Factors and Cybersecurity in NHS Virtual Wards

Theofanis Fotis[1,2], Kitty Kioskli[2,3], and Haralambos Mouratidis[3]

[1]University of Brighton, School of Sport & Health Sciences, Centre for Secure, Intelligent and Usable Systems (CSIUS), Brighton, BN19PH, United Kingdom
[2]Trustilio B.V., Vijzelstraat 68, 1017 HL Amsterdam, The Netherlands
[3]University of Essex, School of Computer Science and Electronic Engineering, Institute of Analytics and Data Science (IADS), Parkside Office Village, Wivenhoe Park, Colchester CO4 3SQ, United Kingdom

ABSTRACT

The rapid evolution of healthcare technology, particularly in the wake of the COVID-19 pandemic, has led to a significant increase in the establishment and expansion of Virtual Wards by the National Health Service (NHS) in the United Kingdom. Virtual wards provide patients with hospital-level care in the comfort of their homes, facilitating quicker recovery while also freeing up hospital beds for those most in need. Patients receive daily reviews by the clinical team, which may involve home visits or virtual ward rounds conducted via video technology. Many virtual wards utilize apps, wearables, and other medical devices to enable clinical staff to easily monitor patients' recovery progress. While this shift extends healthcare services remotely, it also presents cybersecurity challenges inherent to the new infrastructure, particularly concerning human factors of stakeholders involved. This paper will explore the context of NHS virtual wards, focusing on user interface design, usability, and accessibility of virtual ward technologies, and discussing their impact on both patients and healthcare professionals. Special attention will be given to the challenges faced by diverse patient groups, such as the elderly and individuals with disabilities, in navigating virtual healthcare environments, and how these factors influence the vulnerabilities of virtual ward technologies from a human factors perspective. Additionally, this paper will examine regulatory frameworks and standards, the role of patient and staff training in cybersecurity awareness, and the integration of advanced security measures within these new healthcare infrastructures. Emphasizing the importance of a human-centric approach, this work will propose a multi-disciplinary strategy to address these challenges, advocating for privacy-by-design modelling of Virtual Wards and promoting collaboration among patients, healthcare professionals, IT experts, cybersecurity specialists, and policymakers.

Keywords: Virtual wards, Human factors, Cybersecurity, Human centric cyber hygiene, Privacy by design

INTRODUCTION

Over the past decade, the National Health Service (NHS) in the UK has undergone a significant digital transformation journey, driven by the Long-Term Plan initiated in 2019. This plan outlines the NHS's commitment to

© 2024. Published by AHFE Open Access. All rights reserved.

leveraging technology to enhance healthcare delivery over the next decade, highlighting its pivotal role in improving citizen care. As part of this transformation, and in response to the challenges posed by the pandemic, virtual wards have been introduced, also known as "hospital at home" programs, building upon the pioneering "virtual ward" model first utilized in Croydon, south London, in 2004.

These virtual wards employ a multidisciplinary team approach, incorporating remote monitoring technology, regular virtual consultations, and occasional in-person visits from healthcare professionals (Norman et al., 2023). This innovative model offers several benefits, including alleviating strain on hospital resources, empowering patients with greater control over their recovery in familiar surroundings, and potentially expediting healing by reducing exposure to hospital-acquired infections (Taylor & O'Mahony, 2021).

However, the transition to virtual wards presents challenges, particularly in the domains of human factors and cybersecurity, stemming from the new out-of-hospital environment, infrastructural adjustments, supply chain considerations, and the involvement of human stakeholders. On the human factors front, disparities in digital literacy, social isolation, and potential technology dependence among patients necessitate tailored solutions to ensure equitable access and prevent exacerbating existing vulnerabilities. Healthcare professionals must adapt their communication and assessment skills to the virtual environment, effectively fostering relationships and managing patient expectations in situations where physical presence is limited. Moreover, the reliance on technology introduces a new dimension of risk, underscoring the need for robust cybersecurity measures to safeguard sensitive patient data and ensure the integrity of remote care delivery. This includes implementing rigorous network security protocols, providing comprehensive staff training in data protection, and proactively identifying and mitigating potential cyber threats to maintain patient trust and uphold the integrity of the healthcare system.

The aim of this paper is to delve into the realm of NHS virtual wards, with a specific focus on the design, usability, and accessibility of their user interfaces, and to explore their impact on both patients and healthcare professionals. It will particularly address the challenges faced by diverse patient groups, including the elderly and individuals with disabilities, when navigating virtual healthcare environments, and analyze how these challenges influence the vulnerability of virtual ward technologies from a human factors standpoint. Additionally, the paper will examine regulatory frameworks and standards, the importance of patient and staff training in enhancing cybersecurity awareness, and the integration of advanced security measures within these evolving healthcare infrastructures. Emphasizing a human-centric approach, this paper will propose a multi-disciplinary strategy to tackle these issues, advocating for the implementation of privacy-by-design principles in Virtual Wards and fostering collaboration among patients, healthcare professionals, IT experts, cybersecurity specialists, and policymakers.

NHS Virtual Wards Infrastructure

At its core, a virtual ward functions as a hospital-level care unit operating remotely. Patients receive the necessary medical attention while residing in their own homes, or potentially in care homes, fostering a sense of familiarity and comfort during recovery (Carrier & Newbury, 2016). This model typically involves a multi-pronged approach. Remote monitoring technology, employing wearable devices and sensors, captures vital signs and health data in real-time (see Figure 1). Regular virtual consultations, facilitated by secure video conferencing platforms, enable healthcare professionals to monitor progress, adjust treatment plans, and address patient concerns. Additionally, in-person visits provide essential hands-on care and physical assessments, bridging the gap between virtual and traditional modalities.

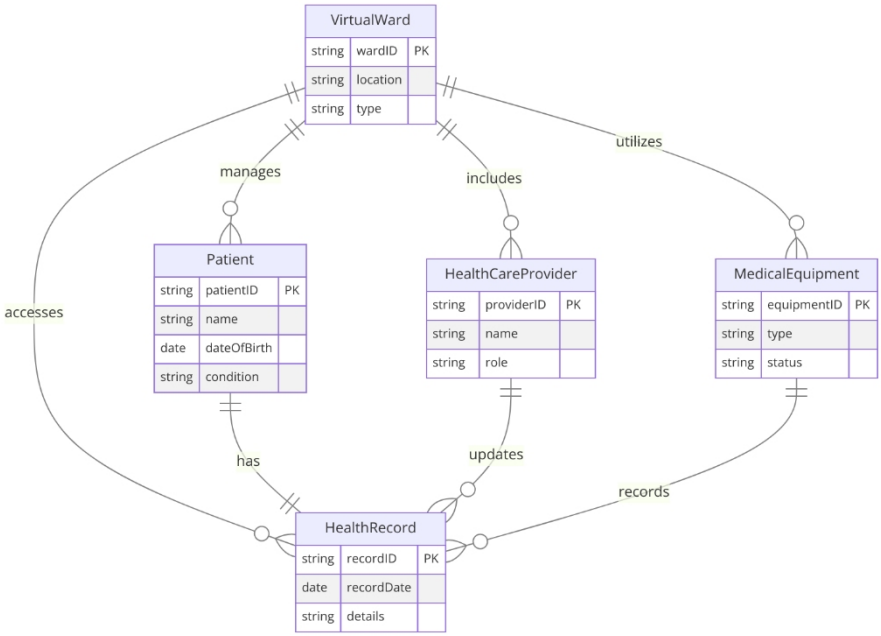

Figure 1: A simple schematic representation of a potential virtual ward.

The genesis of NHS virtual wards can be traced back to the early 2000s, with the Croydon Primary Care Trust pioneering the concept. Initially focused on managing chronic conditions such as chronic obstructive pulmonary disease (COPD), the model gradually expanded to encompass a wider range of medical needs (Guardian, 2007). The COVID-19 pandemic served as a potent catalyst, accelerating the adoption of virtual wards due to their ability to manage patients outside of potentially saturated hospital settings. Today, numerous NHS trusts across the UK implement a diverse array of virtual ward programs, catering to various patient populations and conditions, from post-operative care to managing respiratory infections and supporting individuals with frailty (Elias et al., 2023).

While NHS virtual wards hold the promise of accessible, convenient, and efficient healthcare by shifting the center of care to the patient's home, effectively facilitating this human-computer interaction becomes crucial. In this remote monitoring environment where patients remain in familiar surroundings, user-friendly interface design is the cornerstone of equitable access, optimal care delivery, and ultimately, patient and healthcare professional satisfaction (Henni et al., 2022).

Visual representation of the supply chain of virtual wards can take various approaches. Some platforms may prioritize straightforward functionality, mimicking familiar web interfaces with clearly categorized options and intuitive navigation, while others may adopt a more immersive approach, utilizing gamification elements or personalized dashboards to enhance engagement and self-management. Regardless of the approach, challenges regarding usability remain a persistent concern (see Figure 2).

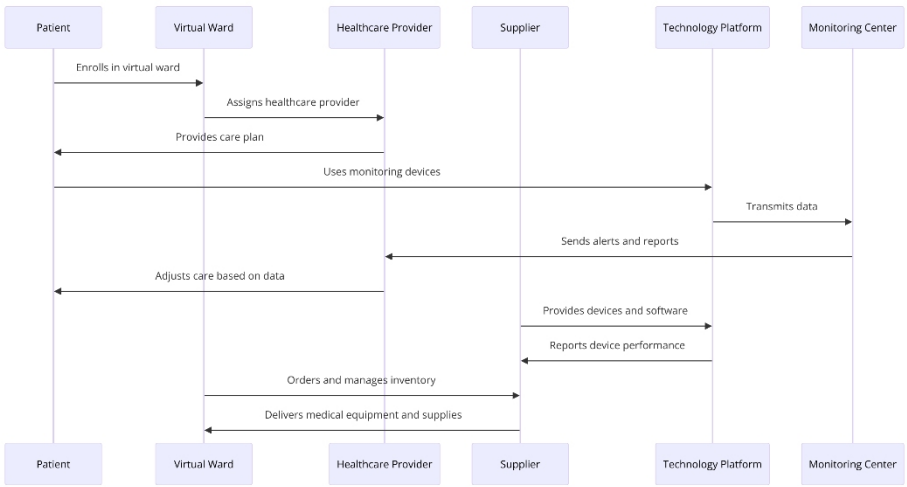

Figure 2: A potential supply chain of a virtual ward.

One major usability hurdle pertains to the inherent complexity of managing health information. Patients, often grappling with anxiety and unfamiliar medical terminology, require interfaces that present data in a clear, concise, and readily understandable manner. Complicated dashboards, excessive jargon, and complex navigation pathways can exacerbate existing anxieties and impede efficient care management. Similarly, healthcare professionals navigating virtual care platforms require efficient data visualization tools, streamlined communication functions, and intuitive workflows to optimize their time and deliver effective care (Brewer et al., 2020; WHO, 2018).

The impact of usability shortcomings can be significant for patients, where frustration and confusion can lead to reduced engagement, missed medication doses, and ultimately compromised health outcomes. These challenges can be exacerbated for elderly patients, individuals with disabilities, and those with limited digital literacy, for whom specific design considerations

are required to ensure equitable access and prevent the widening of existing health disparities (Wadhwa et al., 2019).

Addressing these challenges requires a multifaceted approach through robust usability testing involving diverse patient and healthcare professional demographics to identify and eliminate design flaws. Incorporating user-centered design principles from the outset and involving real end-users in the development process are crucial steps. Ensuring user needs are met at every stage and adopting established accessibility guidelines and best practices in virtual wards are essential for enhancing usability and accessibility (NHS, 2023; Van Kessel et al., 2022).

Virtual Wards, Human Factors and Cybersecurity Vulnerabilities

As virtual wards transform healthcare landscapes, their unique and new supply chain with digital interconnectedness, where medical data, diagnoses, and medication plans are shared through a complex network of devices, platforms, and healthcare professionals, combined with the patient at home, introduces new vulnerabilities and cybersecurity threats (Kioskli et al., 2023; Ntantogian et al., 2021) see Figure 3.

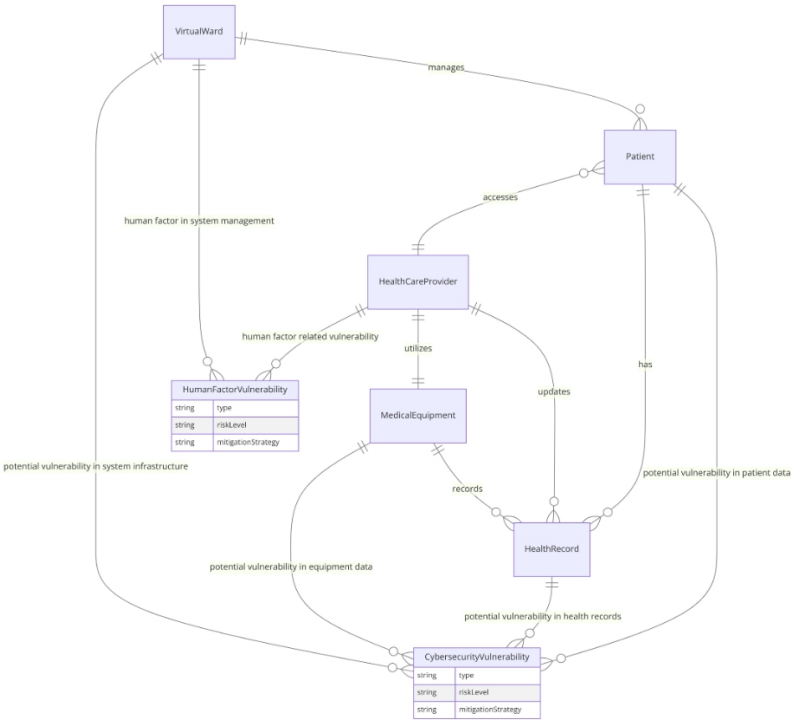

Figure 3: Cybersecurity vulnerabilities in a virtual ward.

Human Factors: The Weakest Link?

While sophisticated technology safeguards are typically present in hospital infrastructures, in a 'hospital at home' setting, the human factor becomes a critical aspect of cybersecurity and may act as the weakest link in the cybersecurity chain. Considering the diverse range of patients at home, several key factors contribute to this vulnerability (Nifakos et al., 2021; Yeo et al., 2022):

1. Lack of Cybersecurity Awareness: Many patients and healthcare professionals may have limited understanding of online threats and safe practices, making them susceptible to phishing attacks and social engineering manipulation.
2. Weak Passwords and Data Sharing: Practices such as password reuse or sharing passwords with relatives and caregivers can provide easy access for attackers. Additionally, casual data sharing through personal email or unencrypted platforms compromises patient privacy and exposes sensitive information.
3. Negligence and Human Error: Simple oversights, such as leaving devices unattended or failing to update software patches, can create exploitable vulnerabilities for malicious actors to exploit.

Addressing these human factors and promoting cybersecurity awareness among patients and healthcare professionals is crucial to mitigating these risks and ensuring the security of 'hospital at home' environments. Measures such as comprehensive cybersecurity training, robust password management policies, and regular security audits can help strengthen the cybersecurity posture of virtual healthcare settings.

Furthermore, relevant studies on human factors influencing cybersecurity compliance among healthcare staff indicate a correlation between work pressure, deficient information security knowledge, and negative information security attitudes with increased Information Security Conscious Care Behaviour (ISCCB) risks. Conversely, healthcare professionals exhibiting greater agreeableness, openness, and those operating within a robust security culture demonstrate reduced likelihood of engaging in risky cybersecurity behaviours. Intriguingly, conscientiousness was unexpectedly associated with higher ISCCB risks and perceived severity of punishment. This finding emphasizes the importance of designing intuitive, workflow-integrated security protocols and providing continuous security education within healthcare environments (Yeng et al., 2022).

Mitigating the Human Factor: Building Cyber Resilient Virtual Wards Through Privacy by Design

Within the healthcare sector, several existing cybersecurity solutions have been deployed. Notable examples include the use of endpoint device management tools, remote work environment security measures, security awareness training, technical controls, and mechanisms for incident reporting and cyber threat intelligence (He et al., 2021). However, these established solutions are primarily implemented within hospital settings and lack rigorous evaluation in out-of-hospital, community-based healthcare contexts, particularly

for novel infrastructures such as the virtual ward models. Given the evolving nature of virtual wards and the absence of established best practices, their cybersecurity status remains under-researched.

Given the diverse stakeholder interactions and inherent complexities within virtual wards, as discussed above, security demands a multi-faceted, customized approach. Privacy by Design offers a promising framework, having demonstrated effectiveness in similarly complex infrastructures (Alkubaisy et al., 2022, Al-Obeidallah et al., 2023). To address the specific security vulnerabilities of virtual wards, we propose the adaptation of a Privacy by Design approach combined with co-designing principles, that encompasses several strategies, including:

- Regular Training: Providing ongoing training for both patients and healthcare professionals to recognize threats, adopt safe online habits, and safeguard sensitive information (Burton et al., 2023).
- Strong Security Measures: Enforcing strong password policies, implementing multi-factor authentication, and utilizing data encryption across all virtual ward platforms and devices.
- Insider Threat Mitigation: Identifying and addressing potential insider threats through background checks, access controls, and ethical training.
- User-friendly Security Integration: Integrating security measures into platforms in a user-friendly manner that doesn't hinder usability.

This multi-pronged approach relies on open communication, shared responsibility, and a collective commitment to privacy by design (Clarke, 2014; Debatin et al., 2020). Patients should be empowered to access, understand, and control their data through intuitive interfaces and transparent policies. Healthcare professionals require training and support to navigate data regulations and implement secure practices. IT experts must prioritize encryption, user authentication, and robust system monitoring. Collaboration between cybersecurity specialists and healthcare professionals is essential for conducting regular risk assessments and vulnerability testing. This collaboration can be shaped further by applying co-design methodologies, where stakeholders collaboratively design and implement solutions (Darley, 2022). By bringing together the patients, the expertise of cybersecurity professionals, IT staff and healthcare professionals and providers, co-design fosters a deeper understanding of security vulnerabilities and user needs. This collaborative approach can lead to the development of more user-friendly and effective security solutions that consider the specific workflows and challenges faced by healthcare personnel. Additionally, co-design empowers all stakeholders to take ownership of cybersecurity practices, fostering a culture of shared responsibility and leading to more sustainable and effective security outcomes. Policymakers, guided by ethical principles and public trust, should establish clear data governance frameworks and hold all stakeholders accountable for data security (Diamantopoulou et al., 2017). See Figure 4 for an illustration of these principles in action.

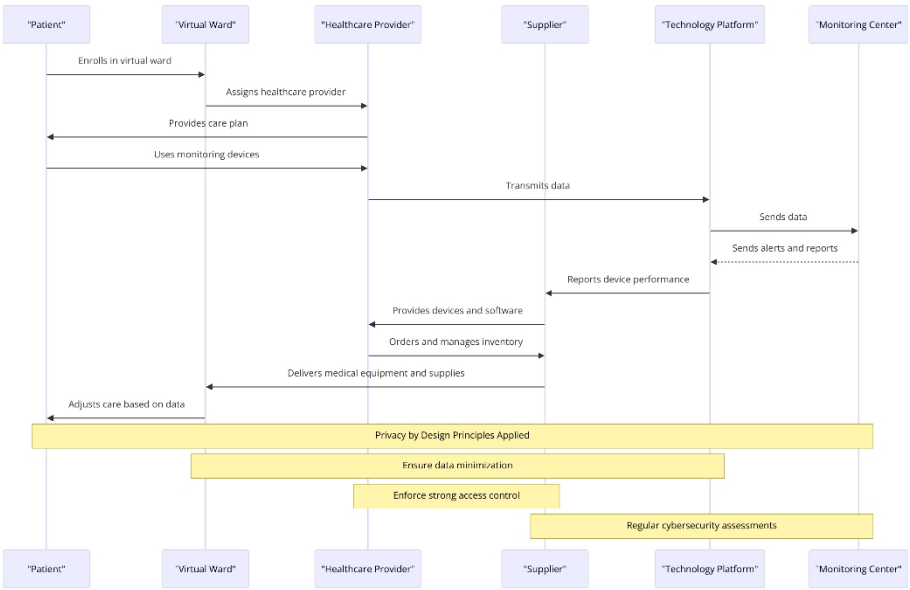

Figure 4: A hypothetical privacy by design approach for a virtual ward.

CONCLUSION

NHS virtual wards represent a remarkable advancement in healthcare delivery, promising to reshape the landscape of patient care. However, the integration of these virtual care settings brings with it a set of cybersecurity vulnerabilities that demand careful consideration and proactive measures. As we move forward, it is essential to recognize and address these vulnerabilities to ensure the safety, security, and effectiveness of virtual ward environments.

Clinical implications abound in the context of cybersecurity vulnerabilities within virtual wards. Patient data security is paramount, and any breach or compromise could have serious consequences for patient confidentiality and trust in the healthcare system. Therefore, clinical practitioners must remain vigilant in implementing robust cybersecurity protocols to safeguard patient information and uphold professional standards of care. Additionally, the potential for cyberattacks to disrupt vital healthcare services underscores the critical importance of maintaining uninterrupted access to patient care, even in the face of digital threats.

Practical implications of addressing cybersecurity vulnerabilities in virtual wards extend beyond the clinical realm. From a practical standpoint, healthcare organizations must invest in comprehensive cybersecurity training for both staff and patients to foster awareness and preparedness for potential threats. Furthermore, the development and implementation of advanced encryption techniques, decentralized data storage models, and artificial intelligence-powered threat detection systems can enhance the security posture of virtual ward environments, bolstering patient trust and confidence in remote healthcare delivery.

Moreover, addressing cybersecurity vulnerabilities in virtual wards holds broader implications for the healthcare system as a whole. By prioritizing the

integration of secure and accessible care practices, healthcare organizations can promote equitable access to healthcare services while mitigating the risk of cyber threats. This, in turn, fosters a healthcare ecosystem that prioritizes patient safety, privacy, and satisfaction, ultimately leading to improved health outcomes and enhanced overall quality of care.

By recognizing the challenges, incorporating diverse perspectives, and prioritizing secure and accessible care, healthcare organizations can navigate the complexities of virtual care delivery while ensuring the safety and well-being of patients. This proactive approach not only safeguards patient data and healthcare services but also fosters trust, confidence, and resilience in the face of evolving cybersecurity threats.

ACKNOWLEDGMENT

The authors would like to acknowledge the financial support provided for the following projects: 'Collaborative, Multi-modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce In the European Digital Single Market and Industries' (CyberSecPro) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No. 101083594. The 'Human-centered Trustworthiness Optimization in Hybrid Decision Support' (THEMIS 5.0) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101121042. The 'advaNced cybErsecurity awaReness ecOsystem for SMEs' (NERO) project, which has received funding from the European Union's DEP programme under grant agreement No. 101127411. And 'Fostering Artificial Intelligence Trust for Humans towards the optimization of trustworthiness through large-scale pilots in critical domains' (FAITH) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101135932. The views expressed in this paper represent only the views of the authors and not of the European Commission or the partners in the above-mentioned projects.

REFERENCES

Alkubaisy, D., Piras, L., Al-Obeidallah, M. G., Cox, K., Mouratidis, H. (2022). A Framework for Privacy and Security Requirements Analysis and Conflict Resolution for Supporting GDPR Compliance Through Privacy-by-Design. In: Ali, R., Kaindl, H., Maciaszek, L. A. (eds) Evaluation of Novel Approaches to Software Engineering. ENASE 2021. Communications in Computer and Information Science, vol 1556. Springer, Cham. https://doi.org/10.1007/978-3-030-96648-5_4

Al-Obeidallah, M., Piras, L., Iloanugo, O., Mouratidis, H., Alkubaisy, D and Dellagiacoma, D. (2023). Goal-modeling privacy-by-design patterns for supporting GDPR compliance. International Conference on Software Technologies (ICSOFT). Rome (Italy) 10–12 Jul 2023 Rome (IT) SciTePress. https://doi.org/10.5220/0012080700003538

Brewer, L. C., Fortuna, K. L., Jones, C., Walker, R., Hayes, S. N., Patten, C. A., & Cooper, L. A. (2020). Back to the future: Achieving health equity through health informatics and digital health. JMIR mHealth and uHealth, 8(1), e14512.

Burton, S. L. (2023). Change management and cybersecurity in healthcare. In Transformational Interventions for Business, Technology, and Healthcare (pp. 426–443).

Carrier, J., & Newbury, G. (2016). Managing long-term conditions in primary and community care. British Journal of Community Nursing, 21(10), 504–508.

Clarke, R. (2014). Big data and the right to privacy: A digital book from the Oxford Internet Institute. Oxford University Press.

Darley, A. and Carroll, Á. (2022) 'Conducting Co-Design with Older People in a Digital Setting: Methodological Reflections and Recommendations', International Journal of Integrated Care, 22(4), p. 18. Available at: https://doi.org/10.5334/ijic.6546.

Debatin, B., Zar, M., & Miller, S. (Eds.). (2020). Privacy in information technology: New directions in research and practice. Springer.

Diamantopoulou, V., Kalloniatis, C., Gritzalis, S., & Mouratidis, H. (2017). Supporting privacy by design using privacy process patterns. In S. De Capitani di Vimercati & F. Martinelli (Eds.), ICT systems security and privacy protection (SEC 2017) (Vol. 502, pp. 33–42). Springer.

Elias, E., Winn, T., Paz, E., et al. (2023). Experience and outcome from a London NHS trust heart failure virtual ward. Heart, 109, A85.

Gill, N., Bennett, P., & Vardy, E. R. L. C. (2023). Virtual wards: A rapid evidence synthesis and implications for the care of older people. Age and Ageing, 52(1), afac319.

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. Journal of medical Internet research, 23(4), e21747. https://doi.org/10.2196/21747

Henni, S. H., Maurud, S., Fuglerud, K. S., et al. (2022). The experiences, needs and barriers of people with impairments related to usability and accessibility of digital health solutions, levels of involvement in the design process and strategies for participatory and universal design: A scoping review. BMC Public Health, 22, 35. https://doi.org/10.1186/s12889-021-12393-1

Kioskli, K., Fotis, T., & Mouratidis, H. (2021). The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations. In Proc. of the 16th International Conference on Availability, Reliability and Security on SecHealth Workshop (ARES'21) (pp. 1–19).

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cybersecurity within healthcare organizations: A systematic review. Sensors, 21(15), 5119. https://doi.org/10.3390/s21155119

NHS. Digital technology. Retrieved from https://www.england.nhs.uk/digitaltechnology/.

Norman, G., Bennett, P., & Vardy, E. R. L. C. (2023). Virtual wards: A rapid evidence synthesis and implications for the care of older people. Age and Ageing, 52(1), afac319. https://doi.org/10.1093/ageing/afac319

Tech-enabled virtual wards: Relieving pressure on the NHS while caring for patients at home. Retrieved from https://transform.england.nhs.uk/key-tools-and-info/data-saves-lives/improving-individual-care-and-patient-safety/virtual-wards-relieving-pressure-on-the-nhs-while-caring-for-patients-at-home/#:~:text=It%20was%20first%20pioneered%20for,at%2092%20sites%20across%20England.

Taylor, D., & O'Mahony, D. (2021). Virtual wards in healthcare: A review of the literature. Journal of Advanced Nursing, 77(10), 3039–3050.

Van Kessel, R., Hrzic, R., O'Nuallain, E., Weir, E., Wong, B. L. H., Anderson, M., & Baron-Cohen, S. (2022). Digital health paradox: International policy perspectives to address increased health inequalities for people living with disabilities. Journal of Medical Internet Research, 24(2), e33819.

Wadhwa, A., & Reddy, S. (2019). User experience and interaction design for e-health systems. Springer Nature.

World Health Organization. (2018). Inclusive digital healthcare: A framework for NHS action on digital inclusion. Retrieved from https://www.who.int/publications/i/item/9789241516570

Yeng, P. K.; Fauzi, M. A.; Yang, B. (2022) A Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals. Information13, 335. https://doi.org/10.3390/info13070335

Yeo, L. H., & Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. Perspectives in health information management, 19 (Spring), 1i.