PEER RESPONSE 1

The WannaCry cyberattack was a significant moment. It showed how much healthcare relies on technology and how quickly time can slip away when systems fail. To prevent this from happening again, it's not just about fixing technical issues; it involves shifting habits and priorities across the board. Let's start with the basics: updates. In 2017, many NHS computers were still running outdated versions of Windows, leaving them vulnerable to attacks. A stricter patch approval system and someone taking charge of non-patching could have greatly reduced the damage (Department of Health and Social Care, 2018).

Next is the human element: We've all accidentally clicked on something suspicious at some point; expecting staff to inherently know better isn't realistic. Regular short training sessions or reminders during shifts could help keep these risks fresh in employees' minds (NHS Digital, 2022). What about effective network design? If key systems are isolated from the rest, an attack on one area doesn't need to affect everything else (National Cyber Security Centre, 2023).

Lastly, plans only work if they're practiced. Running a cyberattack drill might seem strange initially but could save crucial hours during an actual crisis.

REFERENCES

Department of Health and Social Care (2018) Lessons learned review of the WannaCry ransomware cyber attack. London: DHSC. National Cyber Security Centre (2023) Cyber security for healthcare organisations. London: NCSC. NHS Digital (2022) Cyber security in the NHS: Best practice guide. Leeds: NHS Digital.

PEER RESPONSE 2

Firstly, as you mentioned Abdulrahman, patching security vulnerabilities and asset management is extremely important; this can be achieved by maintaining a live inventory of devices (including data on the status of patching and the scale of obsolete technology) and enabling automatic updates where feasible.

The critical importance of establishing rapid emergency patching for critical vulnerabilities is underscored by Smart's (2018) finding that, despite being advised by NHS Digital's CareCERT bulletin, "None of the 80 NHS organisations affected by WannaCry had applied the Microsoft update patch." Furthermore, as you touched on, implementing network segmentation, which divides the network into isolated sections, can significantly mitigate the impact of an attack by preventing the movement of threats through the network, as was seen during the WannaCry attack (McKeon, 2025).

This ensures that if one part of the network is compromised, then the infection can be contained, consequently protecting critical systems and sensitive patient data. In the wake of the cyber-attack, the UK government put in place a plan to enhance cyber resilience across the health and social care sector by 2030, which advocates for embedding security into the design of new technologies and ensuring every organisation is equipped to minimise the impact of an incident (Department of Health and Social Care, 2023).

REFERENCES

Department of Health and Social Care (2023) Government sets out strategy to protect NHS from cyber-attacks. GOV.UK. Available at: https://www.gov.uk/government/news/government-sets-out-strategy-to-protect-nhs-from-cyber-attacks (Accessed: 11 August 2025).

McKeon, J. (2025) Minimizing healthcare cyberattacks with network segmentation. Available at: https://www.techtarget.com/healthtechsecurity/feature/Minimizing-healthcare-cyberattacks-with-network-segmentation(Accessed: 11 August 2025).

Smart, W. (2018) Lessons learned review of the WannaCry Ransomware Cyber Attack. Independent Report. London: Department of Health and Social Care.

PEER RESPONSE 3

Your post provides an excellent overview of how Industry 4.0 and Industry 5.0 intersect with the UK healthcare sector, particularly in the NHS. The example of the WannaCry ransomware attack is powerful because it demonstrates not just a technical vulnerability but also the wider consequences for patient safety and trust. Ghafur et al. (2019) are right to note the economic cost, but the indirect impacts such as delays in treatment and increased stress on staff are equally significant and often harder to quantify.

I think your call for a shift towards Industry 5.0's human-centric model is crucial. Automation and digitalisation cannot replace the empathy, ethical reasoning, and adaptability that healthcare professionals bring. Instead, as Saxena et al. (2024) argue, hybrid models that blend smart technologies with human oversight offer a more resilient and socially responsible path. This aligns with wider research suggesting that effective use of AI in healthcare must include transparent governance and clinician involvement at every stage (Topol, 2019). Another point worth emphasising is cyber resilience.

The WannaCry incident showed how a single cyberattack could cripple vital services. Strengthening NHS digital infrastructure with real-time monitoring, redundancies, and staff training is as important as adopting new technologies. Industry 5.0's focus on collaboration and sustainability offers an opportunity to integrate these safeguards into system design from the outset (Abdel-Basset, Mohamed and Chang, 2025). Overall, your discussion captures well the balance between innovation and human-centred care. The NHS is uniquely placed to demonstrate how Industry 5.0 principles can build not only efficiency but also equity, resilience, and trust in healthcare delivery.

REFERENCES

Abdel-Basset, M., Mohamed, R. and Chang, V. (2025) 'A Multi-Criteria Decision-Making Framework to Evaluate the Impact of Industry 5.0 Technologies: Case Study, Lessons Learned, Challenges and Future Directions', Information Systems Frontiers, 27(2), pp. 791–821.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. and Aylin, P. (2019) 'A Retrospective Impact Analysis of the Wannacry Cyberattack on the NHS', NPJ Digital Medicine, 2(1), p. 98.

Saxena, A., Chauhan, S.P.S., Singh, H., Chauhan, U. and Kumari, P. (2024) 'Impact of Industry 5.0 on Healthcare', Infrastructure Possibilities and Human-Centred Approaches with Industry 5.0, pp. 182–198. ▪ Topol, E. (2019) Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again. London: Basic Books.