

Overlooked and under-reported: the impact of cyberattacks on primary care in the UK National Health Service



Rapid digitisation and interconnectivity of the UK National Health Service (NHS) among hospital trusts, general practices, and patients help to streamline patient care across sectors.¹ However, this increased connectivity also raises the NHS's vulnerability to cyberattacks. Cyber threats targeting health-care systems are increasing on a global scale,² but cybersecurity in health care has not advanced as fast as in other critical sectors such as energy, finance, and transportation. As bad actors become more sophisticated in perpetrating further attacks, discussions regarding the NHS's resilience to cyberattacks have intensified.³

On June 3, 2024, Synnovis, a partnership between SYNLAB (Europe's largest provider of medical testing and diagnostics) employed by Guy's and St Thomas' NHS Foundation Trust and King's College Hospital was hit by a ransomware cyberattack demanding US\$50 million.⁴ The disruption also propagated to the 194 general practice surgeries in southeast London using the Synnovis platform.⁵ The attack caused a complete lockdown of Synnovis's systems, limiting access to pathology services and severely disrupting patient diagnostics, blood transfusion processing, and result reporting.⁶ Final data from NHS England revealed that the disruption led to the cancellation of 10 152 outpatient appointments and 1710 elective procedures being delayed in secondary care at Guy's and St Thomas' NHS Foundation Trust and King's College Hospital. Resolution to near-normal levels was achieved 16 weeks after the initial shutdown.⁴ Reports on the impact of these weeks of downtime have been focused on secondary and tertiary services, and little is known about the impact on primary care.

Approximately 300 million patient consultations take place in general practices every year.⁷ In the Synnovis cyberattack, substantial disruption to pathology services occurred in primary care services across southeast London for several weeks. The inadequate capacity to process blood tests had a downstream effect on these practices, as resources were redirected to prioritise hospital care. Restricted access to pathology services stymied the ability of primary care services to obtain timely test results for new diagnoses and management of patients with chronic diseases and urgent investigations, leaving primary care struggling to address routine and emergent patient needs effectively.

When a cyber incident strikes, the systemic impact is vast, creating a ripple effect across the national health-care infrastructure, hampering patient care.² With the increased propensity of cyberattacks, the impact of these attacks on primary care remains under-reported in terms of its safety and security concerns. Although, in primary care, no patient harm has yet been directly attributed to cyberattacks,⁴ accurately assessing their impact is challenging owing to the complexities involved in quantifying downstream effects. Delays in cancer diagnoses and referrals to secondary care, along with disruptions in managing chronic conditions, could have pronounced, long-term effects on patient outcomes and the delivery of safe care. These consequences, however, remain largely unmeasured and unreported, highlighting the far-reaching implications of extended service disruption.

The WannaCry attack in 2017 highlighted these vulnerabilities; minimal data exist on its specific effect on primary care and general practice services.² National statistics suggest that 595 of 7454 general practices were affected.⁸ The Synnovis attack reveals the ongoing requirement for a resilient health-care system in which all health-care stakeholders recognise the acute need for robust cyber defences. Only through system-wide attention to cybersecurity can the NHS adequately protect patient safety amid increasingly sophisticated cyber threats.

Repeated cyberattacks are exposing vulnerabilities and causing widespread disruption across the NHS. Concerns persist that these attacks are being addressed in isolation, and the recurring cyberattacks on the NHS highlight a broader, systemic issue that demands nationwide attention. The NHS's new cyber assessment framework,⁹ developed by the National Cyber Security Centre, supports health-care organisations in building defences against cyber threats and identifying high-risk areas. The new Labour Government in the UK has recently released details of a Cyber Security and Resilience Bill to strengthen the defences of UK's critical digital infrastructures.¹⁰ Together, these initiatives reflect the Government's commitment to building cyber resilience within NHS England.

Several cybersecurity enhancement plans have been established since the nationwide 2017 WannaCry attack.⁷ No quantifiable insights have been gained regarding the

Lancet Digit Health 2025;
7: 100879

Published Online May 24, 2025
<https://doi.org/10.1016/j.landig.2025.100879>

impact on primary care in WannaCry and Synnovis incidents. As cybercriminals are using increasingly sophisticated techniques such as artificial intelligence and machine learning to automate attacks, evade detection, and exploit vulnerabilities at scale, resilience to cyberattacks should become a priority for every individual within the health-care system. Without understanding the true impact of these attacks on all aspects of health-care systems, resilience plans¹⁰ will continue to be lacking. Similar to the underfunding of primary care highlighted in the independent investigation of the NHS,¹ the under-reporting of the impact of cyberattacks directly correlates with this systemic issue. The NHS's digital transformation and expanded data integration make cybersecurity a crucial, often overlooked, patient safety issue, particularly in primary care.

We declare no competing interests.

Copyright © 2025 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

**Kunal Rajput, Ara Darzi, Saira Ghafur*
k.rajput24@imperial.ac.uk

Institute of Global Health Innovation, Imperial College London, London SW7 2AZ, UK (KR, AD, SG)

- 1 Darzi A. Independent Investigation of the National Health Service in England. September, 2024. <https://assets.publishing.service.gov.uk/media/66f42ae630536cb92748271f/Lord-Darzi-Independent-Investigation-of-the-National-Health-Service-in-England-Updated-25-September.pdf> (accessed Dec 20, 2024).
- 2 Alder S. Healthcare data breach statistics. April 17, 2025. <https://www.hipaajournal.com/healthcare-data-breach-statistics/> (accessed April 20, 2025).
- 3 Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digit Med* 2019; 2: 98.
- 4 National Health Service England. Update on cyber incident: clinical impact in South East London – Thursday 26 September 2024. Sept 26, 2024. <https://www.england.nhs.uk/london/2024/09/26/update-on-cyber-incident-clinical-impact-in-south-east-london-thursday-26-september-2024/> (accessed Dec 20, 2024).
- 5 National Health Service South East London Clinical Commissioning Group. An introduction. April, 2020. <https://moderngov.southwark.gov.uk/documents/s90522/Item%206i%20Appendix%20A%20-%20Introduction%20to%20the%20SEL%20CCG.pdf> (accessed Dec 20, 2024).
- 6 Powis S, Lawson E. NHS blood and transplant amber alert for O type blood. July 25, 2024. <https://www.england.nhs.uk/long-read/nhs-blood-and-transplant-amber-alert-for-o-type-blood/> (accessed Dec 20, 2024).
- 7 National Health Service England. Primary Care. <https://www.england.nhs.uk/five-year-forward-view/next-steps-on-the-nhs-five-year-forward-view/primary-care/> (accessed Dec 20, 2024).
- 8 Smart W. Lessons learned review of the WannaCry ransomware cyber attack. Feb 1, 2018. <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf> (accessed Dec 20, 2024).
- 9 National Cyber Security Centre. Cyber assessment framework. <https://www.ncsc.gov.uk/collection/cyber-assessment-framework> (accessed Dec 20, 2024).
- 10 Department for Science, Innovation and Technology. Cyber security and resilience policy statement. April 1, 2025. <https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement> (accessed April 20, 2025).