Trusted Guide

Healthcare Cybersecurity Foundations: Key IT Security Standards for 2026

Cybersecurity is no longer just a technical consideration, it underpins patient safety and the reliable delivery of healthcare services. As organisations become increasingly dependent on digital systems, from patient records and clinical platforms to payroll and everyday communications, the risks they face continue to evolve.

Ransomware attacks, phishing activity, and weaknesses across the supply chain can quickly disrupt critical services, expose sensitive information, and damage patient trust. Although frameworks like UK GDPR and the Data Security and Protection Toolkit (DPST) establish important standards, cybersecurity is about more than simply meeting compliance requirements. It is fundamental to organisational resilience and the delivery of consistent, high-quality care.

By adopting strong, practical security standards, healthcare organisations can better protect their systems and create an environment where staff are free to focus on what matters most; delivering safe, reliable, and compassionate care. This guide outlines ten essential cybersecurity standards to help strengthen resilience and safeguard patient care.

Pauline Gray

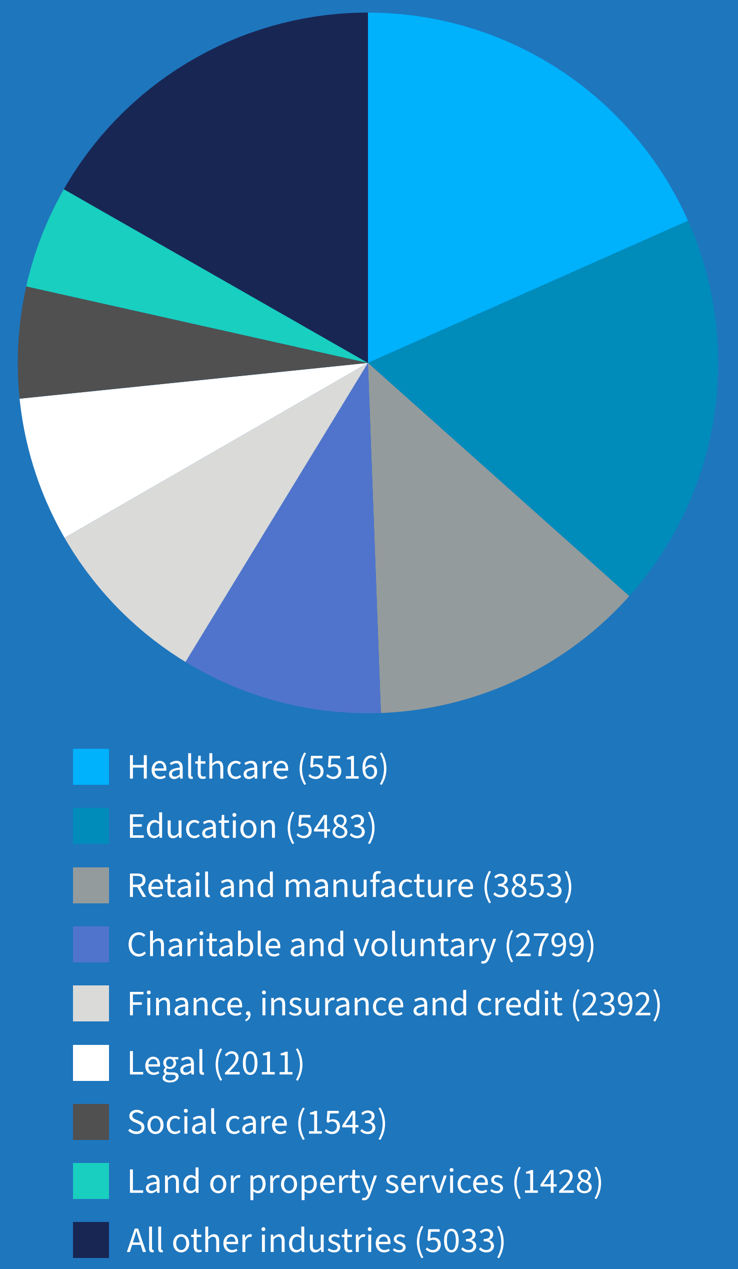
Managing Director
Trusted Technology Partnership

01

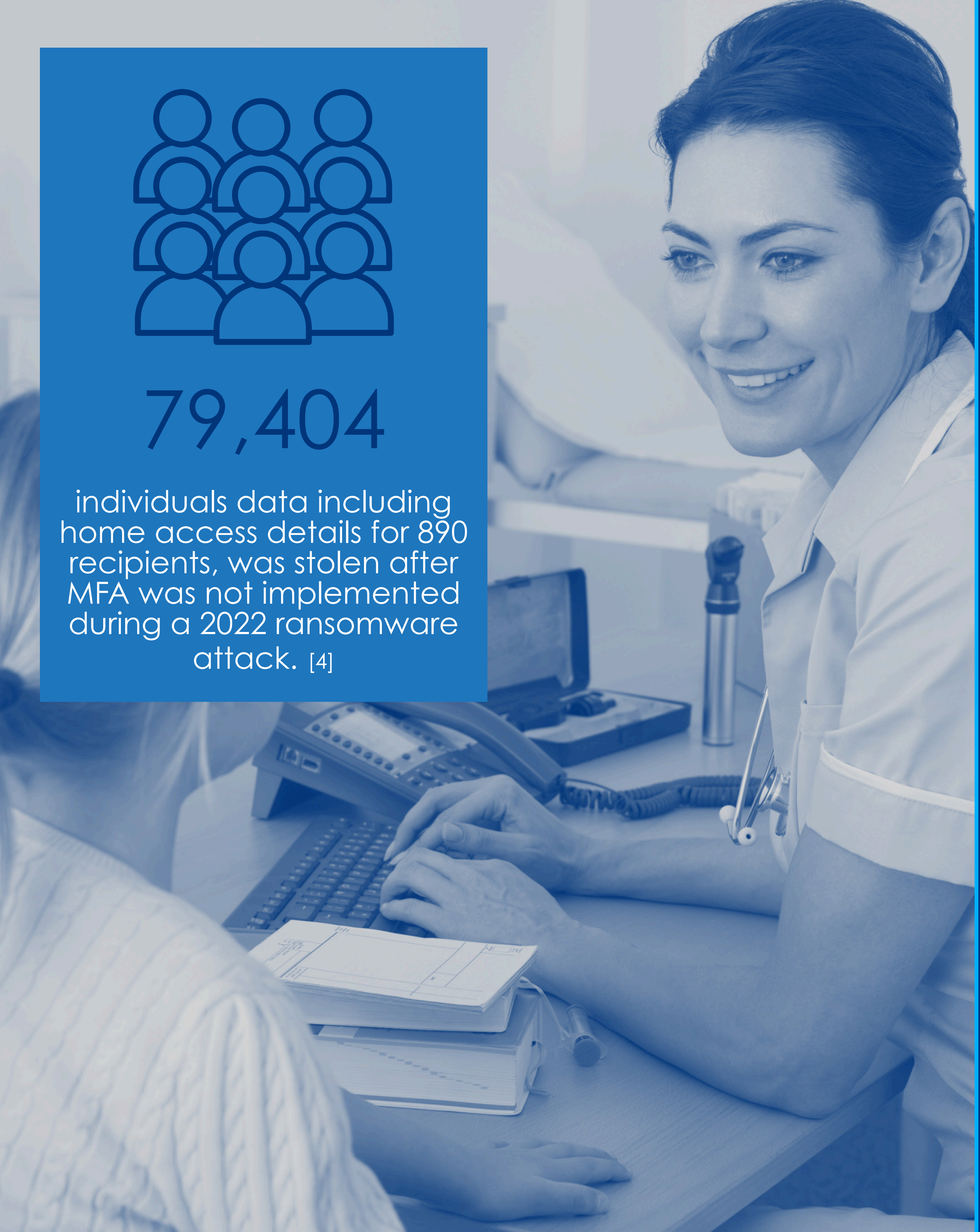
Strong Password Policies

Weak or reused passwords remain a major vulnerability. While many organisations have formal cybersecurity policies, these do not always translate into consistent password habits. The National Cyber Security Centre (NCSC) advises focusing on length and uniqueness rather than overly complex rules, supported by technical measures like password managers [1][2]. Prioritise administrator accounts and remote access, ensuring passwords are regularly updated and never shared between staff.

Data Incidents by Sector [3]



17% of all reported UK data breach incidents in 2024 occurred in the health sector, making it the single most affected industry. [3]



79,404

individuals data including home access details for 890 recipients, was stolen after MFA was not implemented during a 2022 ransomware attack. [4]

02

Multi-Factor Authentication (MFA)

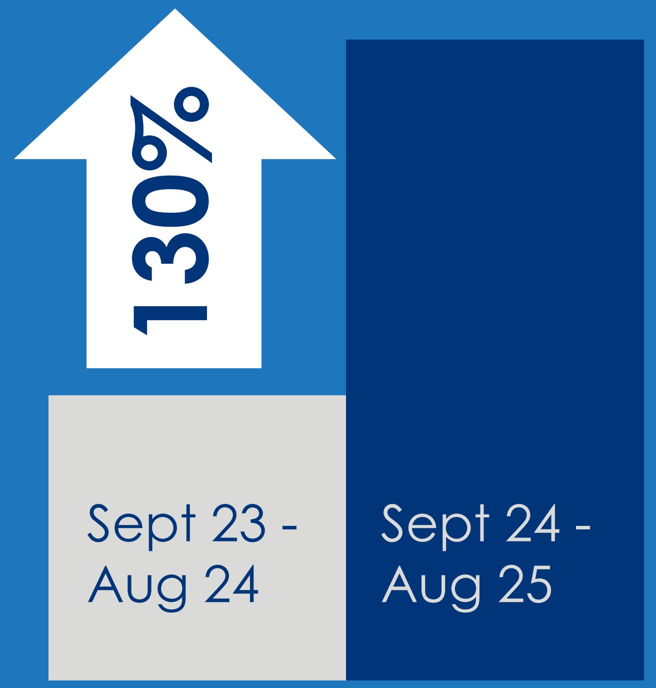
MFA adds an extra layer of protection beyond passwords, making it significantly harder for attackers to gain access even if credentials are stolen. Despite its importance, only around 40% of UK organisations report using MFA in 2025 [5]. For healthcare providers, enabling MFA on care management platforms, payroll systems, and remote access tools is vital. User-friendly options such as app-based verification or biometrics can help overcome usability concerns. Make MFA mandatory for all remote access and administrative accounts, and communicate its role in preventing service disruption.

03

Access Controls

Accounts with extensive access rights should be managed separately from those used for routine tasks like email. Poor control increases the risk of insider threats and accidental changes. Implement role-based access and limit administrative rights to a small group of trusted staff. Review permissions regularly, especially after staff changes, and consider the principle of least privilege [6][7]. For healthcare organisations, this means ensuring clinical staff only have access to the systems they need for care delivery, reducing unnecessary exposure.

41% of UK healthcare organisations reported a cyber breach in 2024 [5].



A notable increase in nationally significant cyber incidents was recorded by the NCSC, with 204 incidents occurring between September 2024 and August 2025. [8]

04

Patching

Unpatched systems remain a critical weakness. Cyber attackers often exploit known vulnerabilities that could have been prevented with timely updates. Follow NCSC guidance to automate updates where possible, prioritise critical patches, and include Internet of Things (IoT) medical devices in your patch cycle [9][10]. Establish a clear patch management policy and monitor compliance across all endpoints, servers, and medical devices. Regular vulnerability scans can help identify gaps before attackers do.

05

Endpoint Protection

Devices used in care settings, laptops, tablets, and mobile phones, are prime targets for malware and ransomware. While most providers use some form of antivirus, gaps in continuous monitoring persist. Deploying Endpoint Detection & Response (EDR) across all devices and centralising management ensures faster detection and response [11]. EDR solutions provide visibility into suspicious activity and allow rapid isolation of compromised devices, reducing the risk of widespread disruption.

71%

of UK organisations report having secure cloud backups in place, yet many healthcare organisations still fail to regularly test restoration processes [5].

3/4

of all breaches involve the human element, including stolen or shared credentials [12].

06

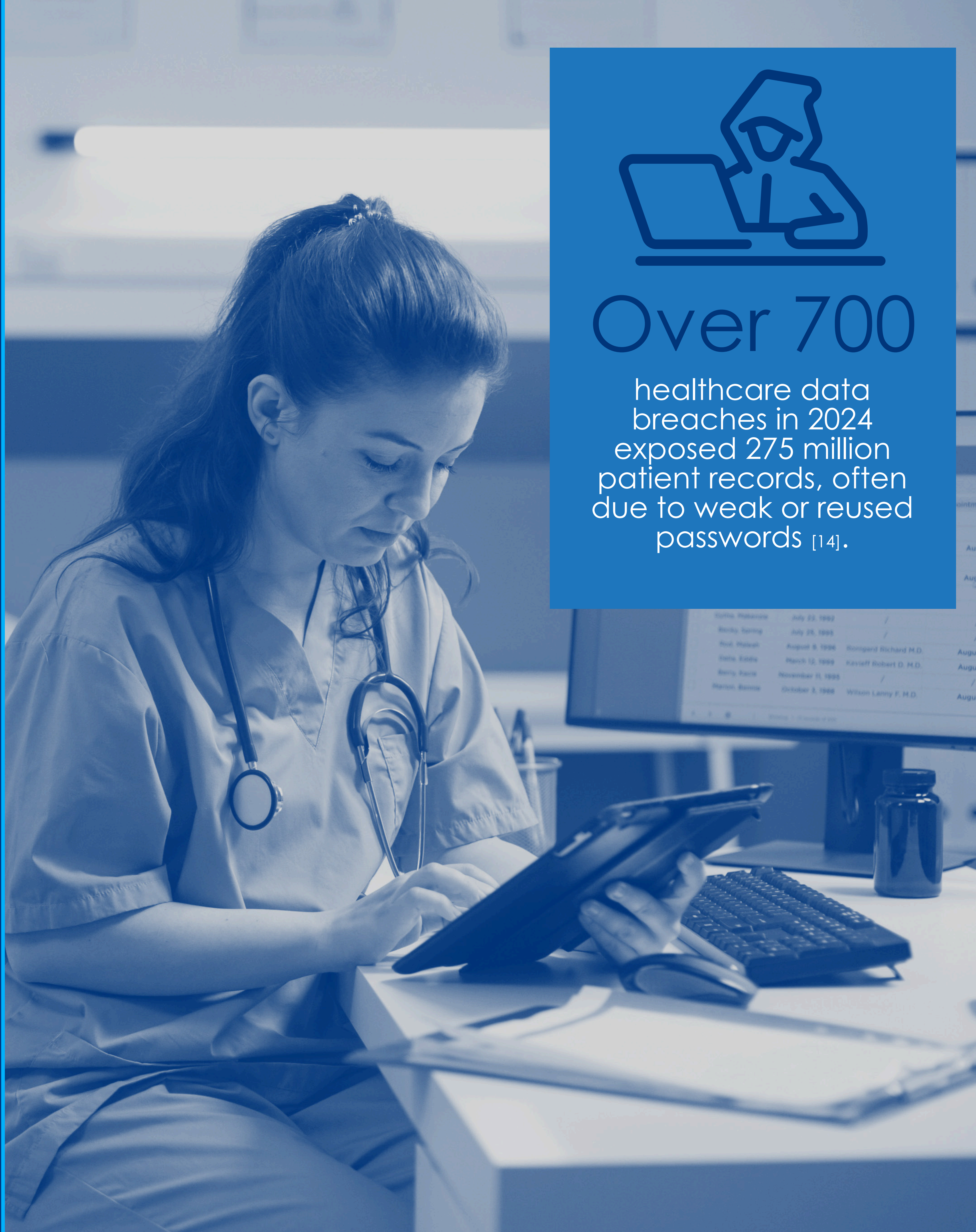
Email & Web Filtering

Phishing remains the most common attack vector, with 85% of breaches involving phishing emails in 2025 [5]. Implementing email and web filtering tools can block malicious links and attachments before they reach staff inboxes. Combined with staff training, these measures significantly reduce risk in environments where email is heavily used for clinical communication and supplier coordination [13]. Consider adding real-time reporting tools so staff can flag suspicious emails quickly, and ensure IT teams respond promptly to reports.

07

Regular Backups

Backups are essential for recovery from ransomware or system failure. Yet many providers lack tested recovery plans. Maintain encrypted backups stored offline or in secure cloud environments and test restoration regularly, including care-critical data like medication schedules and patient records [5]. A backup that hasn’t been tested is a backup you can’t rely on, schedule regular restoration drills and include clinical teams in the process to ensure continuity of care.



Over 700

healthcare data breaches in 2024 exposed 275 million patient records, often due to weak or reused passwords [14].

08

Cybersecurity Training

Human error is a major factor in healthcare cyber incidents, with around 60% of data breaches involving a human element such as phishing or credential misuse [12]. This makes security awareness training more than a compliance requirement, it is essential to building a confident, cyber-resilient workforce. Training should be practical, ongoing, and tailored to care settings, with induction covering core behaviours and regular refreshers reinforced through realistic, healthcare relevant scenarios.

32%

of UK organisations report that cyber security is discussed at board level at least quarterly, highlighting the need for stronger governance in healthcare [15].

09

Supply Chain Risk

Vulnerabilities can quickly compromise your systems. Many providers still rely on trust rather than formal checks when working with technology suppliers. Assess vendor security using frameworks like the DSPT, include cybersecurity clauses in contracts, and monitor compliance regularly [5]. For critical suppliers, such as those providing EPR systems or medication management platforms, require evidence of patching and incident response capabilities.

11,000 +

NHS appointments were disrupted when a ransomware attack on pathology supplier Synnovis shut down critical diagnostic systems [16].

31%

Only 31% of UK organisations have a formally defined incident response plan, despite rising cyber threats to critical services such as healthcare. [5]

10

Incident Response Plan

In healthcare, a clear and well-rehearsed incident response plan is critical to minimising service disruption, protecting patient safety, and reducing reputational harm when cyber incidents occur. Document roles, escalation paths, and regulator reporting steps, and test the plan annually through tabletop exercises [17][18]. Include scenarios such as ransomware, data loss, and denial-of-service attacks, and ensure communication plans cover patients, families, and regulators.

TRUSTED TECHNOLOGY PARTNERSHIP

Your Trusted IT Partner.

For 30 years, Trusted Technology Partnership has supported Healthcare organisations with IT solutions. We understand your focus is on caring for people, we're here to provide the trusted expertise that makes that possible.

🌐 trusted-technology.co.uk

✉ hello@trusted-technology.co.uk

☎ 01425 470888

ISO certified management systems

Certified by ISOQAR - Certificate Number 6172

ISO 9001
ISO 14001
ISO 27001

Certified by Citation- Certificate Number 511482026

ISO 20000

CYBER ESSENTIALS CERTIFIED PLUS

Crown Commercial Service Supplier

EMPLOYEE OWNERSHIP TRUST

Sources

1. NCSC (2025) Password Guidance: Simplifying Your Approach.
2. NCSC (2025) Three Random Words Campaign.
3. ICO (2025) Data Security Incident Trends.
4. ICO (2025) Software provider fined £3m following 2022 ransomware attack.
5. Department for Science, Innovation and Technology (2025) Cyber Security Breaches Survey 2025
6. NCSC (2025) Identity and Access Management Principles.
7. NCSC (2025) Privileged Access Management Guidance.
8. NCSC (2025) NCSC Annual Review 2025.
9. NCSC (2025) Vulnerability Management Guidance.
10. NCSC (2025) Device Security Configuration Baselines.
11. NCSC (2025) Mitigating Malware and Ransomware Guidance.
12. Verizon Business (2025) Data Breach Investigations Report.
13. NCSC (2025) Phishing Attacks: Defending Your Organisation.
14. The HIPAA Journal (2025) Healthcare Data Breach Statistics.
15. NCSC (2025) Board Toolkit: Cyber Risk as Business Risk.
16. NHS (2025) Synnovis Cyber Incident.
17. NHS England (2025) Cyber Incident Response Checklist.
18. ICO (2025) Data Breach Reporting and Incident Handling.