CSBR

Cyber Security and Patient Safety in the NHS

thecsbr.com

The NHS is becoming increasingly dependent on digital infrastructure for safe, timely and effective care.

Contents

Context

The proposed Single Patient Record, wider use of AI, cloud-based systems, and digitally enabled service transformation all have the potential to improve outcomes.

However, they also increase the consequences of cyber failure. Cyber security in health can no longer be treated as a technical back-office issue: it is now a core patient safety, clinical governance and national resilience challenge.

This brief draws on an expert roundtable which was convened by The CSBR, in partnership with The AbedGraham Group, to consider the current state of NHS cyber maturity, the risks created by future digital transformation, relevant international examples, and the practical steps government can take to protect patients from cyber-related harm.

Strategic Priorities

- Cyber security should be recognised explicitly as a patient safety issue, with harm, delay and disruption measured alongside other clinical safety risks.
- The NHS needs a shift from fragmented compliance towards system-wide resilience, including common standards, stronger assurance, and clear accountability from board level to frontline services.
- Future digital reforms, including the Single Patient Record and AI deployment, must be designed around security, resilience, data integrity and clinical continuity from the outset.
- Government should strengthen regulation across the whole health and care ecosystem, including primary care, social care, suppliers, managed service providers and other critical dependencies.
- The NHS should learn from international models that combine leadership accountability, distributed architecture, transparent audit, and routine operational simulation.

The NHS is dependent on a complex network of trusts, primary care providers, social care organisations, suppliers, software vendors, managed service providers, data centres and cloud providers.

Key issues

1. There is no single cyber maturity level

It is structurally misleading to describe the NHS as having a single cyber maturity level. Large acute trusts may have the scale and resources to meet minimum security expectations, but smaller trusts, primary care, social care, community providers and peripheral endpoints often face far weaker baselines. Participants described vulnerabilities ranging from limited use of multi-factor authentication and weak patching to insecure endpoint devices and poor information management practice.

The current model relies too heavily on uneven local capability and self-certification. While investment since WannaCry has improved defensive capability, the NHS still lacks consistent business and clinical resilience. The result is a system that may block more attacks than it did a decade ago but remains vulnerable to disruption that directly affects care pathways.

2. Cyber incidents are already patient safety incidents

Cyber-attacks and digital outages can delay pathology, disrupt emergency care, force diversions, interrupt diagnostics and undermine clinical decision-making. The impact is not limited to data confidentiality. Availability and integrity of clinical systems are equally important. If a record is unavailable, corrupted, maliciously altered or locked by ransomware, the consequences may be measured in delayed treatment, avoidable deterioration and loss of trust.

The NHS lacks a mature, independent framework for reporting and learning from cyber-related harm. Other clinical risks are routinely monitored through safety systems; cyber-related disruption should be treated in the same way. Mortality will often be difficult to attribute directly, so measurement should include morbidity, delayed care, missed treatment windows, cancelled diagnostics, diverted emergency pathways and backlog effects.

3. The Single Patient Record and AI will change the risk profile

A Single Patient Record could improve care coordination, but it also concentrates risk. A unified record increases the consequences of failure in availability, confidentiality or integrity. At the same time, access will remain distributed across a fragmented health and care environment. This means the overall risk profile may be shaped less by the strongest central system and more by the weakest access point.

Widespread AI adoption compounds these challenges. AI can improve detection, triage and defensive cyber capability, but it also creates new attack surfaces, dependency on cloud infrastructure, data sovereignty questions and risks from autonomous cyber threat actors. The NHS should therefore treat AI governance, cyber security, clinical safety and data architecture as a single policy problem rather than separate workstreams.

4. Regulation must cover the whole health and care ecosystem

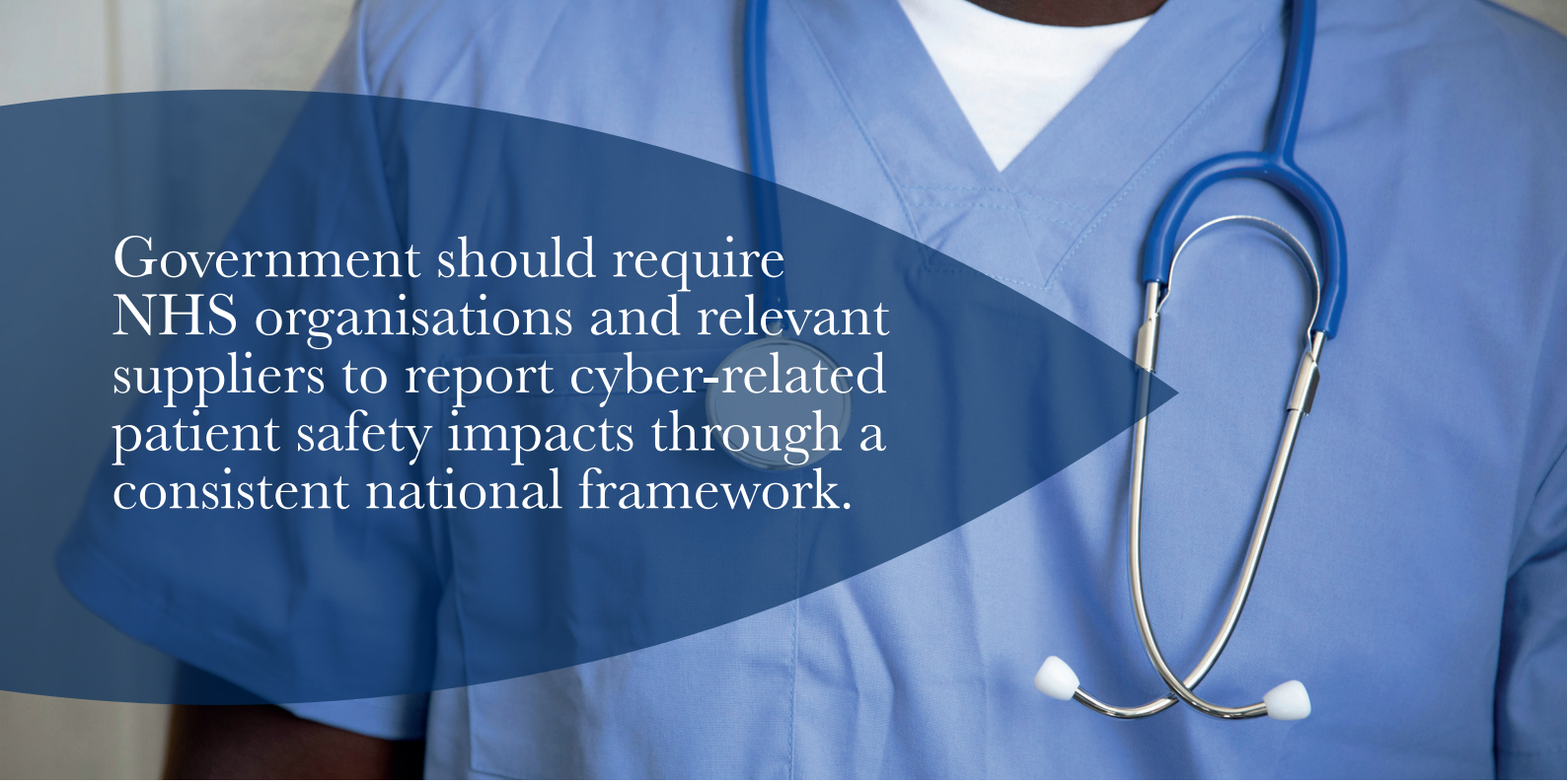
The NHS is dependent on a complex network of trusts, primary care providers, social care organisations, suppliers, software vendors, managed service providers, data centres and cloud providers. A regulatory approach that focuses too narrowly on NHS trusts risks missing the weakest links in the system. Any future regime should apply proportionately across the full chain of clinical dependency.

Minimum standards must not become a ceiling. The government should distinguish between basic compliance, critical national infrastructure resilience, and the higher assurance required for systems whose failure could directly affect patient safety.

5. International examples point to practical lessons

The NHS does not need to start from a blank page. The EU's NIS2 framework highlights the importance of personal leadership accountability. Estonia demonstrates the potential benefits of distributed data architecture and transparent audit of access to records. Singapore and Northern Australia provide examples of strict purpose-based access and operational audit. The Ascension health system in the United States shows the value of organisation-wide cyber simulation and frontline preparedness.

These examples point towards a common lesson: resilience depends on governance, architecture, culture and rehearsal. It cannot be delivered through technology procurement alone.



Government should require NHS organisations and relevant suppliers to report cyber-related patient safety impacts through a consistent national framework.

Policy Themes

1. Establish cyber security as a core patient safety duty

Government should require NHS organisations and relevant suppliers to report cyber-related patient safety impacts through a consistent national framework. This should include delays to treatment, emergency diversions, diagnostic backlogs, cancelled appointments, loss of access to records, data integrity failures and other clinically meaningful harms.

2. Create a stronger central regulatory and assurance function

The government should establish a robust health cyber regulatory and assurance function with the authority to set minimum standards, verify compliance, coordinate regulators, and enforce proportionate obligations across trusts, primary care, social care and critical suppliers. This should be supported by a dedicated health cyber advisory board drawing on clinical, technical, national security and operational expertise.

3. Mandate regular cyber simulation exercises across the NHS

Cyber preparedness should be rehearsed in the same way as major incident response. Government should mandate regular tabletop and live operational exercises covering digital blackouts, ransomware, loss of pathology systems, emergency department disruption and supplier failure. These exercises should include frontline clinicians, managers, digital teams, suppliers, regional leaders and national decision-makers.

4. Use DCB0129 as the bridge between clinical safety and cyber resilience

Government should explicitly connect future NHS cyber security legislation and assurance requirements to DCB0129, the national clinical risk management standard for manufacturers of health IT systems. As DCB0129 is an NHS England information standard published under section 250 of the Health and Social Care Act 2012 and sits alongside DCB0160 for deployment and use, it provides an existing clinical safety mechanism through which technology suppliers can evidence that hazards, mitigations and residual risks have been managed throughout the product lifecycle. Future reforms should keep this standard closely tethered to cyber resilience obligations so that clinical safety, software assurance and cyber security evolve together rather than as separate regimes. Done well, this could position the NHS as a global benchmark for clinically grounded cyber assurance in healthcare technology.

5. Build security and resilience into the Single Patient Record from the start

The Single Patient Record should not proceed as a purely centralised database project. Government should assess a hybrid model combining central assurance, federated interoperability and decentralised repositories. Before deployment, it should resolve digital identity, access control, auditability, data integrity, failover, recovery and clinical continuity requirements.

6. Strengthen accountability at board and senior leadership level

Cyber resilience should be a board-level responsibility linked to clinical safety, not delegated solely to IT teams. Senior leaders should be required to demonstrate understanding of cyber risk, assure preparedness, and take responsibility for organisational resilience. Government should consider how lessons from NIS2-style leadership accountability could be adapted for the UK health and care context.

7. Treat AI governance, cyber resilience and data sovereignty as linked issues

AI deployment in the NHS should be subject to lifecycle governance, clinical validation, cyber assurance, data protection, data sovereignty and clear operational accountability. Defensive AI tools should be explored as part of a broader cyber resilience strategy, but they should not substitute for basic hygiene, leadership, architecture and rehearsal.What form of leadership accountability would be appropriate for NHS boards and senior executives?

Questions for Further Consideration

- Should cyber-related harm be formally incorporated into NHS patient safety reporting frameworks?
- How should regulation apply across trusts, primary care, social care and suppliers without creating disproportionate burdens?
- How should DCB0129 and DCB0160 be updated or linked to future NHS cyber security legislation so that clinical safety and cyber assurance obligations remain aligned?
- What level of assurance should be required before the Single Patient Record is deployed at scale?
- How should government balance data avxailability, confidentiality and integrity in future health digital policy?

Conclusion

The NHS is entering a period of profound digital transformation. The benefits of AI, shared records and digitally enabled care will only be realised if patients, clinicians and the public can trust that systems are secure, resilient and recoverable. Cyber security must therefore be framed as a patient safety imperative. The government should use forthcoming reforms to build a coherent health cyber resilience regime that is proportionate, clinically grounded and designed around the realities of a fragmented health and care system.

July 2026


CSBR


The AbedGraham Group
Clinically Optimized Success