

Hidden Dependencies

Supply-chain cyber risk across healthcare and the public sector

Understanding how interconnected digital services are reshaping operational risk for the NHS and its partners

The challenge facing healthcare

Modern healthcare depends on a dense, invisible web of digital suppliers – from clinical systems and cloud platforms to laboratories, device manufacturers, logistics providers and outsourced service teams. This interconnectedness delivers speed and innovation. It also creates a new form of systemic cyber risk. An incident affecting one supplier can cascade across hospitals, GP networks, laboratories, emergency services and national infrastructure. The result is not just data loss – it is operational disruption.

What we are seeing across healthcare and the public sector

Recent intelligence highlights three dominant patterns:

Supply-chain targeting is increasing

Attackers are deliberately targeting third-party providers in order to reach multiple organisations at once.

Critical services share the same digital dependencies

Blood services, patient record systems, diagnostic platforms and logistics providers often sit on overlapping technology and suppliers.

Disruption, not just data theft, is now the goal

The most damaging incidents increasingly affect service availability and patient care, not only information security.

Why this matters to NHS and public-sector leaders

Cyber risk is no longer isolated to the organisation that is attacked. It is now a procurement issue, a clinical safety issue, a resilience issue and a regulatory issue. Understanding who you depend on, and how exposed they are, has become essential to maintaining continuity of care.

Moving from visibility to control

Questionnaires and point-in-time audits cannot keep pace with live supply-chain exposure.

Orpheus uses real-time threat intelligence to map and score supplier risk across complex ecosystems.

Healthcare leaders gain visibility of critical dependencies and evidence of proportionate, active governance.

Regulatory Accountability

The UK Cyber Security and Resilience Act requires essential services to understand and manage supply-chain cyber exposure.

Orpheus enables NHS Trusts to demonstrate compliance in practice – through continuous supplier visibility, concentration risk identification, and defensible, independently validated risk scoring aligned to board-level accountability.

Explore third-party and supply-chain cyber risk



Speak to Orpheus



About Orpheus

Orpheus provides independently validated cyber-risk intelligence for organisations that depend on complex supplier ecosystems.

We support healthcare and public-sector bodies, insurers and brokers, critical national infrastructure, and procurement and risk teams.

Smarter intelligence.

Stronger outcomes.