



MediShield

The Healthcare Resilience Decision Mapping Tool

This decision mapping flowchart is designed to guide healthcare organisations through a **structured, defensible response to a cyber incident**, from initial detection through to post-incident review. It should be used in real time during an incident.

We have provided recommended time frames but suggest ensuring these are discussed with the relevant teams to ensure they align with your organisations risk appetite and incident response playbook. Every decision gate should be answered deliberately and documented. The purpose is **not just operational clarity, but accountability**: each decision ensures that patient safety, regulatory obligations, and system integrity are properly considered before moving forward.

During an incident, the Incident Lead (typically CIO, IT Director, or designated Incident Manager) should coordinate progression through the phases while assigning clear departmental ownership at each step. The actions in each phase do not need to happen sequentially and instead it is suggested they are completed in tandem.

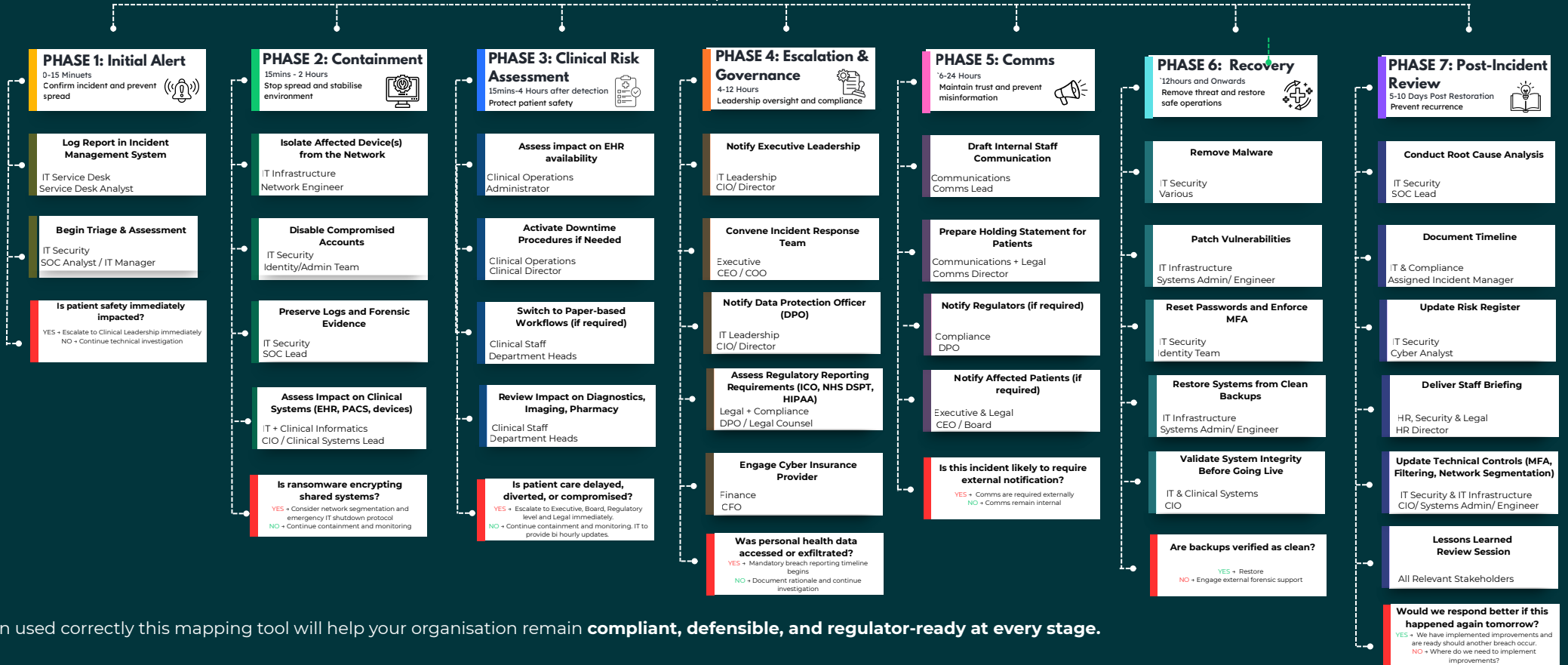
Clinical leadership must be involved early to assess patient safety impacts, and the Data Protection Officer (DPO) must be consulted promptly where personal data may be involved. All decisions, especially those relating to ICO reporting timelines (within 72 hours where required) should be recorded to provide a clear audit trail.

This flowchart is not a substitute for professional judgment; rather, it is a structured framework to provide clarity on unclear responsibilities. It should be reviewed annually, incorporated into tabletop exercises, and aligned with your organisation's broader governance, business continuity, and regulatory compliance framework. When used correctly, it supports **calm, coordinated, and compliant incident management**, protecting patients, staff, and organisational trust.

The Healthcare Resilience Decision Mapping Tool

Because in healthcare, resilience isn't optional, it's duty of care.

Detection

When used correctly this mapping tool will help your organisation remain **compliant, defensible, and regulator-ready at every stage.**

By clearly mapping departmental responsibilities, escalation timelines, and decision gates, it ensures you meet critical obligations, including UK GDPR breach assessment, ICO reporting within 72 hours where required, and documented decision-making that stands up to scrutiny.

At MediShield, our mission is simple: to safeguard patient care by strengthening healthcare cybersecurity governance. We believe compliance should not feel reactive or overwhelming, it should be structured, calm, and built into the fabric of your organisation. Through practical frameworks, clear decision mapping, and regulatory-aligned guidance, MediShield empowers healthcare providers to respond confidently, protect sensitive data, and prioritise patient safety even under pressure.