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.

MediShield

The Healthcare Resilience Decision Mapping Tool

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

Detection

PHASE 1: Initial Alert
0-15 Minuets
Confirm incident and prevent spread

- **Log Report in Incident Management System**
  IT Service Desk
  Service Desk Analyst
- **Begin Triage & Assessment**
  IT Security
  SOC Analyst / IT Manager
- **Is patient safety immediately impacted?**
  YES → Escalate to Clinical Leadership immediately
  NO → Continue technical investigation

PHASE 2: Containment
15mins - 2 Hours
Stop spread and stabilise environment

- **Isolate Affected Device(s) from the Network**
  IT Infrastructure
  Network Engineer
- **Disable Compromised Accounts**
  IT Security
  Identity/Admin Team
- **Preserve Logs and Forensic Evidence**
  IT Security
  SOC Lead
- **Assess Impact on Clinical Systems (EHR, PACS, devices)**
  IT + Clinical Informatics
  CIO / Clinical Systems Lead
- **Is ransomware encrypting shared systems?**
  YES → Consider network segmentation and emergency IT shutdown protocol
  NO → Continue containment and monitoring

PHASE 3: Clinical Risk Assessment
15mins-4 Hours after detection
Protect patient safety

- **Assess impact on EHR availability**
  Clinical Operations Administrator
- **Activate Downtime Procedures if Needed**
  Clinical Operations
  Clinical Director
- **Switch to Paper-based Workflows (if required)**
  Clinical Staff
  Department Heads
- **Review Impact on Diagnostics, Imaging, Pharmacy**
  Clinical Staff
  Department Heads
- **Is patient care delayed, diverted, or compromised?**
  YES → Escalate to Executive, Board, Regulatory level and Legal immediately.
  NO → Continue containment and monitoring. IT to provide bi hourly updates.

PHASE 4: Escalation & Governance
4-12 Hours
Leadership oversight and compliance

- **Notify Executive Leadership**
  IT Leadership
  CIO/ Director
- **Convene Incident Response Team**
  Executive
  CEO / COO
- **Notify Data Protection Officer (DPO)**
  IT Leadership
  CIO/ Director
- **Assess Regulatory Reporting Requirements (ICO, NHS DSPT, HIPAA)**
  Legal + Compliance
  DPO / Legal Counsel
- **Engage Cyber Insurance Provider**
  Finance
  CFO
- **Was personal health data accessed or exfiltrated?**
  YES → Mandatory breach reporting timeline begins
  NO → Document rationale and continue investigation

PHASE 5: Comms
`6-24 Hours
Maintain trust and prevent misinformation

- **Draft Internal Staff Communication**
  Communications
  Comms Lead
- **Prepare Holding Statement for Patients**
  Communications + Legal
  Comms Director
- **Notify Regulators (if required)**
  Compliance
  DPO
- **Notify Affected Patients (if required)**
  Executive & Legal
  CEO / Board
- **Is this incident likely to require external notification?**
  YES → Comms are required externally
  NO → Comms remain internal

PHASE 6: Recovery
`12hours and Onwards
Remove threat and restore safe operations

- **Remove Malware**
  IT Security
  Various
- **Patch Vulnerabilities**
  IT Infrastructure
  Systems Admin/ Engineer
- **Reset Passwords and Enforce MFA**
  IT Security
  Identity Team
- **Restore Systems from Clean Backups**
  IT Infrastructure
  Systems Admin/ Engineer
- **Validate System Integrity Before Going Live**
  IT & Clinical Systems
  CIO
- **Are backups verified as clean?**
  YES → Restore
  NO → Engage external forensic support

PHASE 7: Post-Incident Review
5-10 Days Post Restoration
Prevent recurrence

- **Conduct Root Cause Analysis**
  IT Security
  SOC Lead
- **Document Timeline**
  IT & Compliance
  Assigned Incident Manager
- **Update Risk Register**
  IT Security
  Cyber Analyst
- **Deliver Staff Briefing**
  HR, Security & Legal
  HR Director
- **Update Technical Controls (MFA, Filtering, Network Segmentation)**
  IT Security & IT Infrastructure
  CIO/ Systems Admin/ Engineer
- **Lessons Learned Review Session**
  All Relevant Stakeholders
- **Would we respond better if this happened again tomorrow?**
  YES → We have implemented improvements and are ready should another breach occur.
  NO → Where do we need to implement improvements?

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.