complus

Healthcare providers
IT & Cyber Resilience Checklist

A practical checklist for healthcare organisations and clinical services

MANAGE. PROTECT. ASSURE.

www.complus-it.com

info@complus-it.com

Purpose of This Checklist

IT and Cyber Readiness for Healthcare Organisations

Healthcare organisations rely on secure, reliable systems to support patient care, clinical operations, and sensitive data handling. Gaps in IT or cyber controls can disrupt services, expose patient information, and impact care delivery.

Why this checklist matters

- Clinical and operational systems must remain accessible
- Patient and research data requires strict protection
- Staff access systems across multiple locations and devices
- Downtime can directly affect care delivery

Where Risk Commonly Appears

Most incidents arise from operational weaknesses rather than sophisticated attacks.

- Phishing and credential compromise
- Inconsistent device security across staff
- Excessive or outdated system access
- Backups assumed to work but not tested
- Limited visibility across systems and suppliers

MANAGE

Operational IT Control for Healthcare Environments

Use this checklist to review whether your IT environment reliably supports clinical and operational activities without disruption.

IT Systems & Access

- Clinical and operational systems are clearly identified and supported
- Secure access is available across sites and remote locations
- User access reflects clinical or operational role

Devices & Oversight

- Devices accessing systems are centrally managed and kept up to date
- Personal device use follows a defined policy
- System changes and updates are applied consistently

Support & Accountability

- IT ownership and escalation paths are clearly defined
- Support response times reflect operational priorities

❗ Why this matters

Unstructured IT environments increase the risk of downtime during critical care delivery.

PROTECT

Patient Data, Identity, and System Security

Use this checklist to assess whether patient data and user identities are adequately protected from misuse or compromise.

Data & Access Protection

- Patient and research data is securely stored and access-controlled
- Access is restricted to clinical and operational need
- Data is protected across cloud and on-premise systems

Identity & Email Security

- Multi-factor authentication is enforced on key systems
- Phishing and impersonation threats are actively reduced
- User credentials are protected against compromise

Device & Threat Protection

- Endpoint protection covers all devices
- Lost or stolen devices can be remotely secured
- Security alerts are monitored and reviewed

❗ Why this matters

Weak identity and access controls remain a primary cause of healthcare data incidents.

ASSURE

Continuity, Recovery, and Care Delivery Resilience

Use this checklist to review whether your organisation can continue delivering care and recover quickly during disruption.

Backup & Recovery

- Critical systems and data are backed up securely
- Backup restoration is tested periodically
- Recovery processes are documented

Operational Resilience

- Key systems have defined recovery priorities
- Downtime planning considers patient safety
- Incident response responsibilities are clearly assigned

Why this matters

Untested recovery and unclear response processes increase risk to care delivery and organisational trust.

Your Resilience Snapshot

What This Checklist Reveals

This checklist provides a practical view of how well your IT and cyber environment supports safe, reliable healthcare operations.

It helps you identify whether:

- Clinical and operational systems support care delivery without disruption
- Patient and research data is adequately protected
- User access and identities present avoidable risk
- Devices are consistently managed across staff
- Backup and recovery processes are dependable
- Your organisation can continue operating during IT or cyber incidents

A deeper review may be appropriate if:

- Working patterns or service delivery models have changed
- Systems, platforms, or suppliers have evolved
- Access to patient data is widely distributed
- Backup and recovery have not been tested recently

Next Step

If you would like a second opinion

This checklist is intended as a starting point. If you would like an independent view of your IT and cyber resilience, Complus IT can provide structured guidance aligned with healthcare operations.

How to get in touch

Email
info@complus-it.com

Address
32 Threadneedle St. London, EC2R8AY