ASIAN SCHOOL OF CYBER LAWS

Cyber Security Checklist for Hospitals and Healthcare: 20 Questions to Ask

Tick each question you can answer with a confident yes. Every unticked box is a place to start.

VISIBILITY

01 ☐ Do we have an inventory of every connected medical device and its software version?

02 ☐ Do we know which suppliers we depend on for clinical care?

03 ☐ Do we know every remote access route into our network?

ACCESS

04 ☐ Is MFA enforced on every remote access portal, VPN and email account?

05 ☐ Do help desks verify identity strongly before resetting passwords or MFA?

06 ☐ Are administrator accounts separate, limited and monitored?

NETWORK

07 ☐ Are medical devices on separate network segments from office IT?

08 ☐ Are building systems and guest Wi-Fi separated from clinical systems?

09 ☐ Are internet-facing systems patched quickly?

DETECTION

10 ☐ Do we monitor our network around the clock?

11 ☐ Would we spot an attacker moving inside the network before ransomware is deployed?

12 ☐ Would we notice large amounts of patient data leaving the network?

RESILIENCE

13 ☐ Are backups of clinical systems stored offline and tested?

14 ☐ Could we deliver safe care on paper for two weeks or more?

15 ☐ Do we have contingency plans if a key supplier, such as our lab, goes down?

RESPONSE

16 ☐ Is a cyber attack part of our hospital's major incident plan?

17 ☐ Have we agreed who decides on diversions and cancellations?

18 ☐ Have we run a downtime exercise with clinical staff in the last 12 months?

PEOPLE AND GOVERNANCE

19 ☐ Have staff been trained to spot phishing and phone scams?

20 ☐ Does the board treat cyber risk as a patient safety risk?