



Patient care can't run on unsupported devices

Your device estate is now a clinical risk.



The risk is real

- The 2017 WannaCry attack hit at least 80 of 236 NHS trusts, forcing the cancellation of around 20,000 appointments and operations by exploiting unpatched Windows systems.
- Healthcare currently has the highest share of remaining Windows 10 devices of any sector.¹
- Patient data breaches via unpatched endpoints carry ICO reporting duties within 72 hours and increase enforcement risk.

What's at stake

The 2025/26 NHS Data Security and Protection Toolkit (DSPT v8) is aligned to the NCSC Cyber Assessment Framework, requiring mandatory independent audits for Category 1 and 2 organisations.

DSPT guidance is explicit that no unsupported operating systems should be used within the IT estate. With submission deadlines on 30 June each year, unsupported Windows 10 devices are an audit finding waiting to happen.

Featured XMA Solutions

XMA partners with vendors such as Microsoft to provide highly secure Copilot+ PCs tailored for clinical environments.

- **XMA Clinical Mobile Solution:** A lightweight Copilot+ device offering all-day battery life to support community care without disruption.
- **XMA Ward Workstation:** A reliable Copilot+ PC featuring local AI processing to ensure patient data remains on-device and fully compliant.

Why XMA?

XMA holds public sector credentials and operates across relevant procurement frameworks. We provide deployment and imaging services designed specifically for large healthcare estates.

[Book a device estate review today](#)

Get in touch

 www.xma.co.uk

 enquiries@xma.co.uk

 @xma

 @WeAreXMA

