

3-Step Guide for Securing Personal Mobile Devices

IN HEALTH AND SOCIAL CARE



Your staff **are** using their personal smartphones to share confidential data.

But follow these 3 easy steps and you can close security gaps, and prevent a data breach - without slowing them down. Crisis averted.

Studies have revealed that around **75-80%** of healthcare professionals are using emails, calls, WhatsApp and texts on personal mobile device to discuss patient care. Most do not use dedicated GDPR-compliant messaging services.*

It may provide fast, effective communication within teams, but this widespread reliance on unsecured channels raises serious risks.

Unsecured personal devices are wide open to:

- ✓ **Phishing scams** that trick staff into exposing patient data
- ✓ **Unsecured WiFi** that lets attackers steal NHS login credentials
- ✓ **Malware-infected apps** that can secretly record conversations and steal data

A single device breach could lead to GDPR violations, NHS contract penalties, and patient trust loss. That's why you need a multi-layered approach to mobile security.

Sound daunting? It doesn't have to be!

Follow these 3 simple steps to **protect your workforce's devices without slowing them down.**

1 Harden devices with MDM & MAM

2 Educate users on mobile security

3 Secure devices with MTD



31%

of Healthcare users were targeted with at least one phishing attack **each quarter** in 2022

Lookout data, 2022

1 Harden devices with MDM & MAM

The risks to your organisation:

- ✗ A lost or stolen phone could **expose patient records**
- ✗ Staff use **weak passwords** or store sensitive data in unsecured apps
- ✗ BYOD devices **aren't managed** — leaving security gaps

How to fix it:

✓ Use MDM for Corporate-Owned Devices

Enforce encryption, remote lock, and app restrictions so patient data stays secure.

✓ Use MAM for BYOD

Instead of controlling personal phones, MAM secures just the work apps (e.g., NHS email, patient portals).

✓ Enforce NHS Security Policies

Require strong passwords, automatic screen locks, and up-to-date operating systems.

But here's the catch. MDM and MAM only control access — they don't stop cyber threats. **That's why you need Step 2.**



2 Educate users on mobile security

The primary threats to staff mobile devices are:

- ✗ **Phishing emails and SMS** trick staff into sharing NHS passwords
- ✗ **Fake login pages** steal credentials without them knowing
- ✗ **WhatsApp and personal email** are used for patient discussions — without encryption

How to fix it:

✓ **Phishing Simulations**

Test how well staff recognise real and fake NHS login emails.

✓ **Mobile Security Awareness**

Train employees to spot fake links, malicious apps, and risky WiFi connections.

✓ **Instant Alerts & Coaching**

Use security tools that warn staff in real-time if they click a malicious link.

But even the best-trained employees still make mistakes.

That's why you need Step 3.

3 Secure devices with MTD

The risks to devices:

- ✗ MDM & MAM **don't stop** phishing, malware, or Wi-Fi threats
- ✗ Hackers target NHS workers with **fake login pages**
- ✗ Personal devices **connect** to insecure hospital WiFi

How to fix it:

✓ Phishing & Malware Protection


Automatically block fake NHS login pages, malicious links, and infected apps.

✓ WiFi Risk Detection

Warn staff if they're connecting to a compromised hospital or public Wi-Fi network.

✓ Zero-Trust Security

If a phone is compromised, block it from accessing patient data.

 **MTD acts as your safety net** – catching threats that MDM & MAM can't.

	MTD	MTD + MDM or MAM	MDM or MAM
Protection against phishing	✓	✓	-
AI-powered malware protection	✓	✓	-
Cyber Essentials mobile compliance	✓	✓	-
Zero-Trust access to company data	✓	✓	-
Remote configuration of mobiles	-	✓	✓
Remote app management and installation	-	✓	✓