



# Shared-use mobile devices: Insights, risks, and solutions for UK healthcare

## Executive summary

Mobile technology has become foundational to healthcare in the United Kingdom, driven by the need to improve communication, efficiency, and security. Furthermore, harnessing the power of shared-use mobile devices and ensuring rapid and enthusiastic adoption amongst clinicians will be essential to realising the changes outlined in the [NHS 10-year Plan](#) and the NHS Scotland Digital Health and Care Strategy. But how to do so?

The 2025 Imprivata State of Shared Mobile Devices in Healthcare Report draws upon contributions from 400 health professionals across four countries for real-world insights into maximising ROI, minimising risk, and improving both care delivery and staff satisfaction.

This spotlight report focuses on key takeaways from UK survey respondents. For global figures and more in-depth insights, [check out the full report](#).

## Clinical and IT benefits

Mobile devices are strategic clinical tools that also drive significant IT benefits. Not only do 85% of UK respondents confirm that mobile devices are essential in care settings, but 98% expect the use of shared mobile devices to increase in the next two years.



From the **clinical perspective**, the top benefits driving this increase are:

- Improved communication and coordination among clinical staff (67%)
- Standardisation of workflows across teams (56%)
- Increased flexibility and mobility for staff (56%)



From the **IT perspective**, the top benefits are:

- Greater visibility into mobile device usage and accountability (69%)
- Enhanced asset management, including locating lost devices (65%)
- Increased alignment with compliance and regulations (65%)

## Proven ROI and financial value

85% of respondents believe shared-use mobile devices deliver a greater ROI than individually allocated or BYOD mobile programmes. UK facilities save an average of £522,000 annually using shared devices, but this is still below the global average of £840,000

This gap likely stems from the fact that organisations with a fully implemented shared mobile strategy see a 31% greater ROI than those without – yet in the UK, nearly half (47%) of organisations still lack such a strategy. Consequently, challenges remain that impede greater success.

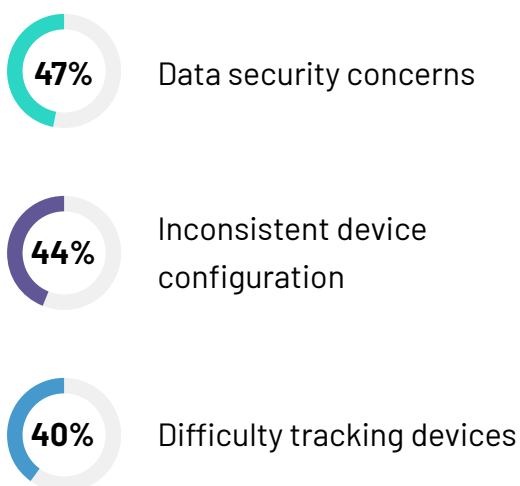
**“These days our whole life is managed on-the-go with mobile. Our clinical colleagues want the same advantages, and our jobs are to ensure that happens safely and securely. The benefits when we get this right are phenomenal.”**

– Andy Kinnear, former NHS CIO, now independent consultant

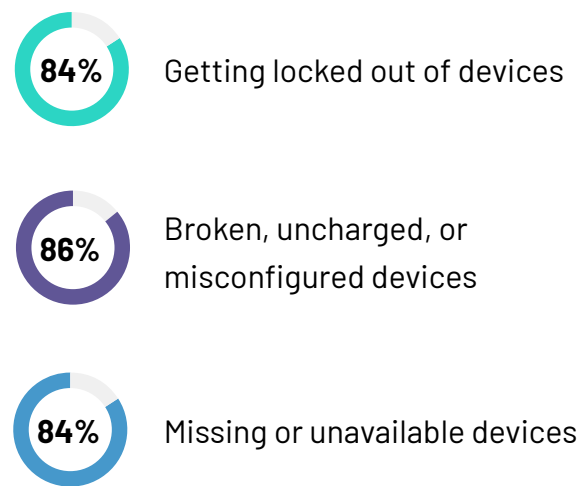
## Challenges in shared mobile device management

Despite the clear benefits of shared mobile, there are a number of challenges that must be addressed to optimise success.

### Operational challenges



### Clinical pain points



**“Since these devices are shared and used by multiple staff throughout the day, we often find ourselves in situations where the device is low on power right when it’s needed most. It can slow down patient care when you have to search for a replacement device or charge it.”**

- Healthcare IT executive, 1,000+ bed facility

## Security and data privacy risks

Without a comprehensive and consistent shared mobile management strategy, privacy risks become a major concern. In fact, 55% of healthcare leaders are not confident that patient data is fully secure on shared devices. The reasons include:



**Staff sharing log-in credentials (reported by 77% of organisations)**



**Devices frequently left signed in (reported by 74%)**



**Personal devices often used as a workaround (reported by 78%)**

Furthermore, security issues are exacerbated when organisations lack the technology to track devices, leading to increased loss and theft. On average, facilities lose 13% of mobile devices annually (approximately 28 devices per facility per year). In addition to the direct costs, survey respondents report that this causes delays in communication (48%), reduced productivity (48%), and increased security risks (48%).

**“We’re finding that using shared mobile devices in the hospital often creates data security concerns. Multiple users accessing the same device can leave patient data exposed if proper logout procedures aren’t followed. It’s a real issue for us.”**

- Healthcare IT executive, 750-999 bed facility

## The future of mobile for UK healthcare organisations

While 44% of respondents say that care team members are reluctant to use mobile devices due to workflow frustrations, this figure is substantially below the global average of 57%. This indicates that most UK healthcare professionals recognise how mobile devices, when made user-friendly, have tremendous potential to drive efficiencies and improve patient care.

To fully unlock the value of shared-use mobile devices, organisations must:

1. Implement **policy-enforced, identity-driven access**
2. Deploy **real-time tracking tools** for device visibility
3. Automate **device provisioning and auditing**
4. Standardise **shift-handover and authentication processes**

As the NHS moves toward more proactive and potentially decentralised models of care, technology will serve as the force multiplier that makes the transformation possible. Shared mobile devices, when properly managed, unlock maximum value for Trusts working under resource pressures. Equipped with the right interfaces, these devices empower clinicians with faster, more intuitive workflows that facilitate better patient experiences and outcomes.

**Download [The 2025 Imprivata state of shared mobile devices in healthcare report: Insights, risks, and solutions](#), to explore the complete dataset and more actionable insights.**





Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. Imprivata's platform of innovative, interoperable access management and privileged access security solutions enable organisations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

**Global headquarters USA**

Waltham, MA

**Phone:** +1 877 663 7446

[www.imprivata.com](http://www.imprivata.com)

**European headquarters**

Uxbridge, England

**Phone:** +44 (0) 208 744 6500

[www.imprivata.com/uk](http://www.imprivata.com/uk)

**Germany**

Langenfeld

**Phone:** +49 (0) 2173 99 385 0

[www.imprivata.com/de](http://www.imprivata.com/de)

**Australia**

Melbourne

**Phone:** +61 3 8844 5533

Copyright © 2025 Imprivata, Inc. All rights reserved. Imprivata is a registered trademark of Imprivata, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.