imprivata®

The 2025 Imprivata state of shared mobile devices in healthcare report: Insights, risks, and solutions

Executive letter

Dear Healthcare Leaders,

At Imprivata, we've long been committed to empowering healthcare organizations with secure and streamlined digital workflows. The rapid advancement of mobile technology has transformed the clinical environment, but it's how that technology is deployed, managed, and maintained that determines its true value.

That's why we launched the *2025 Imprivata state of shared mobile devices in healthcare report.* This report goes beyond surface-level adoption statistics to examine the real-world impacts, both good and bad, of shared-use mobile devices on healthcare organizations and clinical staff. While shared device environments offer significant operational advantages and cost savings in comparison to 1:1 or BYOD (bring-your-own-device) mobile environments, they also introduce unique access, security, and operational challenges.

Our goal with this report is to give IT and clinical leaders data-driven insights that help maximize ROI, minimize risk, and improve both care delivery and staff satisfaction. With contributions from 400 professionals across four countries, this report is a comprehensive look at where the industry stands — and where it must go.

Sincerely,

Dr. Sean Kelly
Chief Medical Officer and Sr. VP of Customer Strategy, Healthcare, Imprivata

Introduction

Mobile devices are no longer just a convenience in healthcare; they are a vital tool for delivering comprehensive and coordinated patient care. These devices can help clinicians access applications, streamline communication, and manage the patient care journey in real time.

In the *2025 Imprivata state of shared mobile devices in healthcare report*, the number of respondents who agree that mobile devices are essential tools in healthcare facilities is now up to **92%.** But an even deeper shift is occurring: the rise of enterprise-owned mobile devices that are used and shared by various employees across shifts and departments, as opposed to dedicated-user devices.

This change is driven by efficiency and cost-savings. Facilities save **$1.1 million annually** by choosing shared-use devices over individually-allocated ones. And almost universally, decision-makers expect this model to grow, with **99%** of respondents anticipating an increase in shared-use devices over the next two years.

Yet the transition to shared devices is not without challenges: access inefficiencies, policy gaps, and security concerns persist. **Sixty-two percent** of respondents said that care staff often experience issues accessing shared-use mobile devices, and **23%** of these devices are lost annually—a staggering statistic with costly implications.

Key findings

92%

of all respondents agree that **mobile devices are essential** tools in care facilities, and 99% expect the use of **shared mobile devices** in their care facility to **increase**

Mobile device use as a clinical tool in care facilities is here to stay

$1.1m

On average is currently **saved every year** by care facilities using shared-use mobile devices (instead of dedicated user mobile devices)

Shared-use mobile devices bring tangible savings for care facilities

62%

Of all respondents say that **care staff experience issues** with accessibility of shared-use mobile devices somewhat, or very, often

Care facilities struggle to make shared-use devices consistently user-friendly

23%

Of shared-use mobile devices **are lost** annually in respondents' care facilities, on average

Many are struggling to manage their shared-use mobile devices, with many using manual processes to assign or to track them

Methodology

For this report, researchers surveyed 400 leaders from acute care facilities with 100+ beds across the United States, Canada, the United Kingdom, and Australia. The respondent pool consisted of 242 IT decision makers and 158 clinical leaders.

SURVEY OBJECTIVES:

- **Assess** current adoption and usage of shared-use mobile devices
- **Explore** benefits across clinical, operational, and security domains
- **Identify** key challenges and barriers to effective implementation of shared-use mobile devices

What's inside

- The benefits of shared-use mobile devices from IT and clinical perspectives
- Workflow challenges, particularly regarding device and application access
- Device management challenges that create operational and security issues

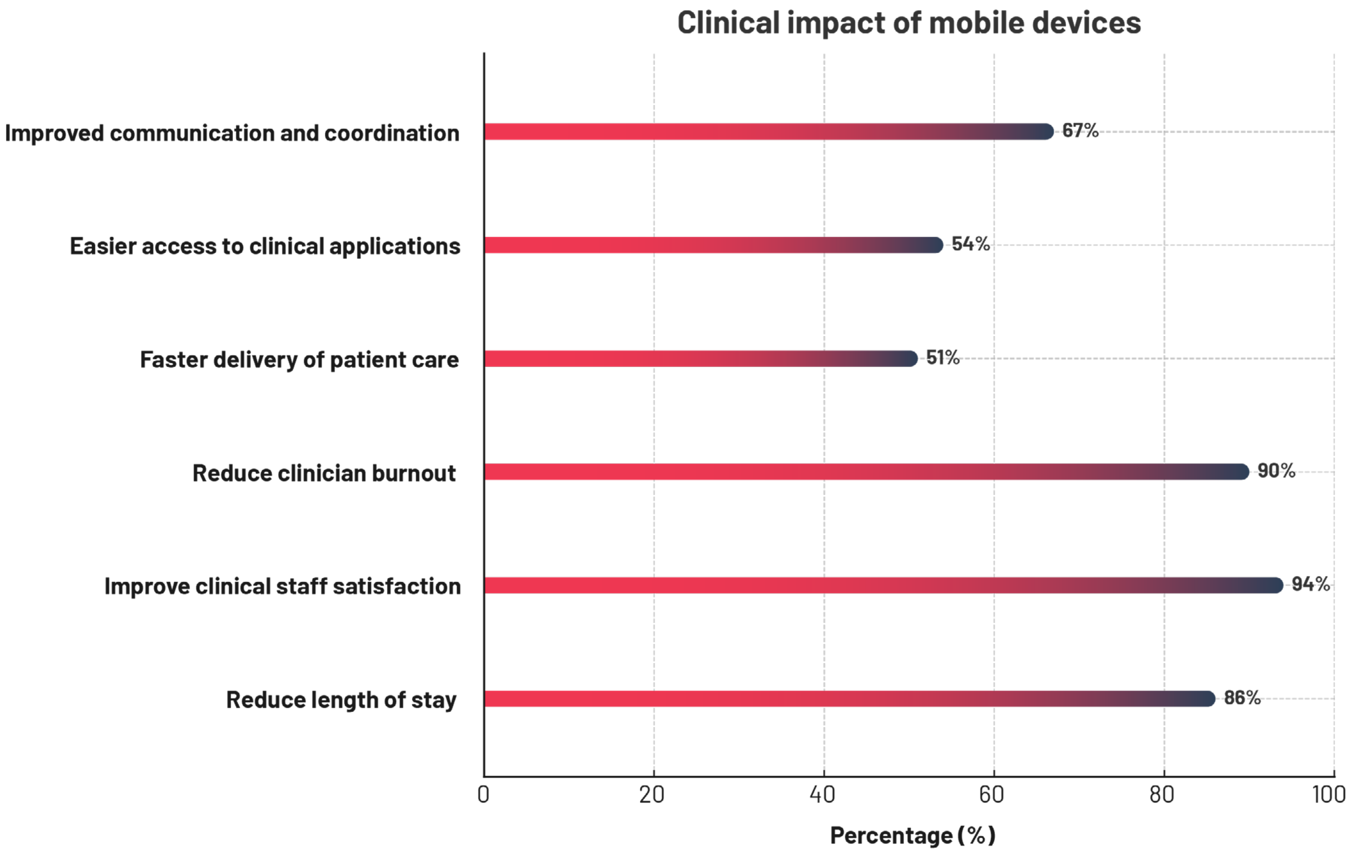
Key findings and statistics

The business case for shared mobile devices

Shared-use mobile programs are not just cost-effective; they are clinically and operationally transformative. First off, mobile device programs, whether shared or not, are a boon to any healthcare organization. **One hundred percent of respondents** agree that care teams experience benefits from using mobile devices in clinical workflows, and **94% agree** that mobile devices facilitate the delivery of high-quality patient care.

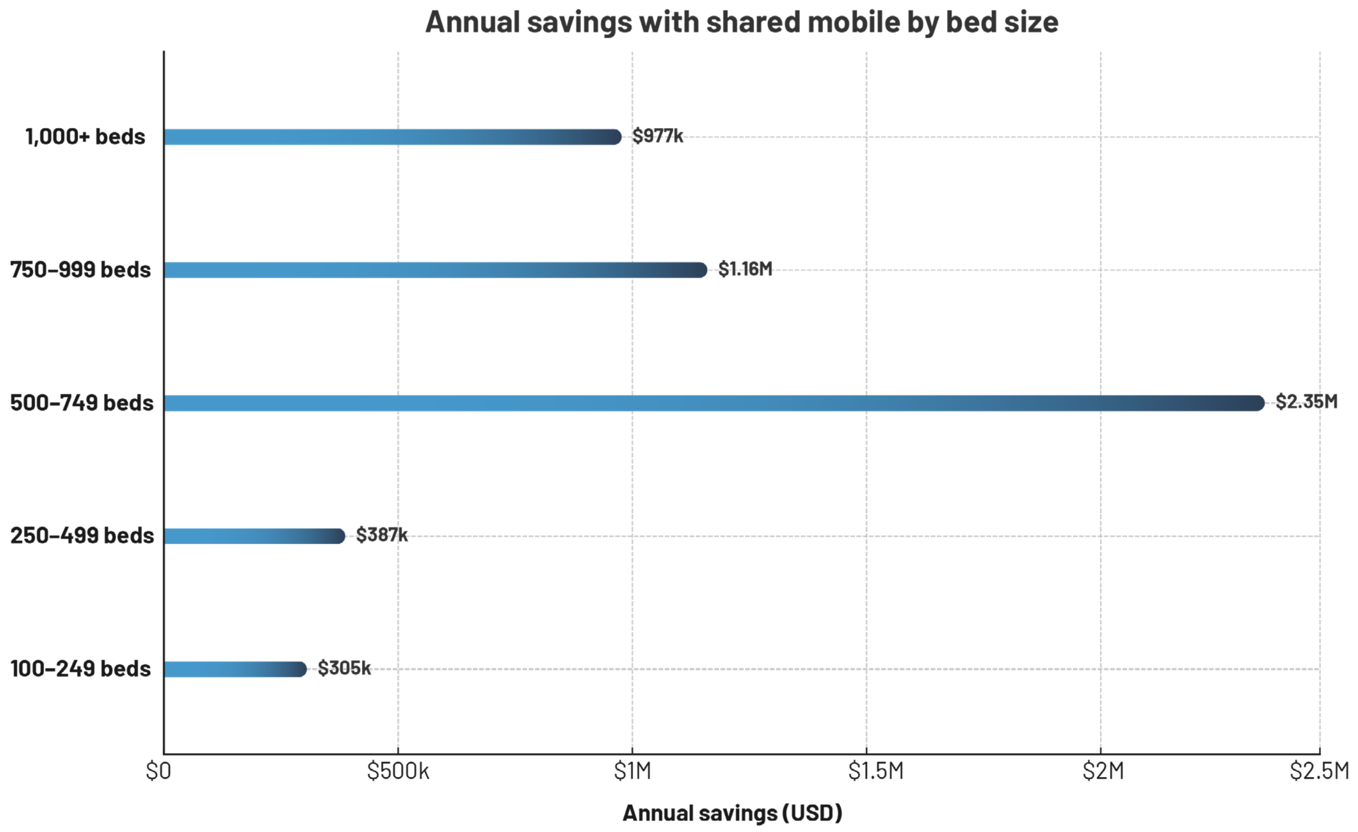
From a clinical perspective, the top benefits of using mobile devices include **enhanced coordination and communication (67%), improved access to clinical applications (54%), accelerated patient care (51%), and faster documentation (46%).** Furthermore, **84%** of respondents agree that the use of mobile devices decreases time to care, and **86%** agree that mobile device use can help reduce the length of patient stays.

Mobile devices also offer substantial intangible benefits, with **90%** of respondents stating that mobile device use saves time and reduces burnout for overworked clinicians, and **94%** stating that mobile devices improve satisfaction among clinical staff.



Shared-use mobile programs elevate these mobile benefits to make them significantly more impactful. For IT teams, shared mobile devices reduce manual workload, which frees them to focus on more engaging, high priority projects that deliver high value to the organization. The top benefits of shared mobile devices for IT teams include **improved asset management in locating lost devices (66%), increased alignment with regulations and compliance (65%), enhanced data security (60%), and greater visibility into mobile device usage and accountability (59%).**

When compared to dedicated-user devices, shared-use devices also provide considerable cost savings. When comparing shared-use mobile devices to 1:1 or BYOD devices, **92%** of survey respondents agree that shared devices deliver greater ROI. In fact, responses showed that by choosing to invest in shared mobile, organizations reap an average annual savings of more than **$1.1 million.**



Considering the sizable cost savings, it is no surprise that **nearly all respondents (99%)** expect their use of shared mobile devices to increase over the next 12–24 months, with **over half (51%)** anticipating a significant increase.

The value of a fully implemented mobile strategy

And yet, despite the many benefits of a well-managed shared mobile device program, **44%** of respondents say their care facility does not have a fully implemented policy for managing their shared-use mobile devices. As a result, those organizations face workflow, operational, and security challenges, while the ROI from mobile investments suffers.

Shared mobile devices result in cost savings in many ways. However, organizations with a fully implemented shared device policy report a **63%** greater ROI than those without a fully implemented policy — **an average annual savings of $1.4 million versus an average annual savings of $860k.**

44%

of respondents say their care facility does not have a fully implemented policy for managing their shared-use mobile devices.

> **“A lack of unified mobile device management tools prevents us from enforcing consistent access controls and data usage policies facility-wide.”**
>
> – IT decision maker, 750 - 999 bed facility, U.S.

Survey respondents are well-aware of the importance of shared mobile access management, with **99%** saying improvement is needed in how access to applications and data is controlled at their organizations. Similarly, **95%** of respondents say improvement is needed with respect to auditing device usage.

Workflow and access challenges

A significant majority of survey respondents (87%) reported experiencing access issues with shared-use mobile devices. Common access frustrations include outdated authentication methods, with **26%** still primarily relying on usernames and passwords for mobile applications.

> **“We struggle with implementing efficient yet secure user authentication methods on shared devices, as frequent login/out processes can be cumbersome.”**
>
> – IT decision maker, 1,000+ bed facility, Canada

But access delays are only part of the story. Productivity losses often begin before a shift even starts due to device assignment challenges. **It takes an average of 13 minutes to assign a shared-use mobile device to a care team member.** The reasons for this include limited availability of mobile devices **(40%),** time-consuming handover processes between shifts **(39%),** use of manual or legacy processes for allocation **(35%),** inconsistent policies or procedures for device assignment **(35%),** and low battery/charge **(35%).**

> **“Security slows everything down. Every time a different nurse picks up a device, they need to re-authenticate. Good for safety, sure, but when you’ve got a code blue, nobody wants to fumble with passwords.”**
>
> – IT decision maker, 1,000+ bed facility, Australia

Overall, **86%** of respondents said that clinical users face challenges with devices being available for use, which in turn hampers communication and delays patient care delivery. Even when devices are provisioned, workflow challenges persist. For example, **87%** percent of respondents cited access challenges such as getting locked out of a device, and **86%** reported usability issues such as devices being broken, not charged, or lacking the right applications and tools.

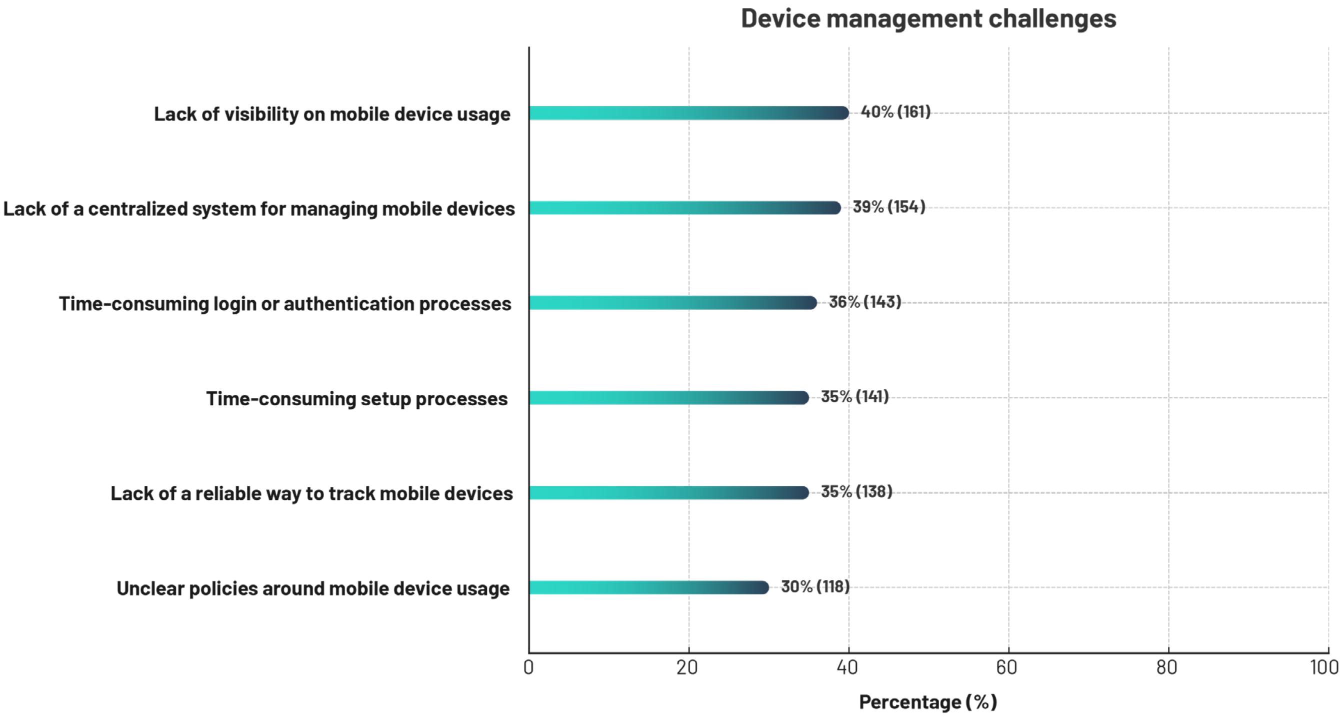
Additional workflow challenges faced by clinical users include inconsistent configuration of applications **(39%)** and time-consuming device authentication processes **(36%).** Unfortunately, when shared-use devices are unavailable or difficult to access, **81%** of respondents say that personal devices are often used instead. This workaround undermines an organization's investment in shared-use devices and limits ROI, while adding new attack vectors that threaten security and create HIPAA compliance concerns.

> **"Imprivata helps us break down adoption barriers and make the most of our mobile technology investments. Checking out a shared device couldn't be simpler. You just tap your badge, pull a phone, log in, and you're good to go. And with the identity-driven approach, staff members can get in touch with the right person, quickly and easily, which is extremely important in an emergency situation."**
>
> – Chris Paravate, Chief Information Officer, Northeast Georgia Health System

Device management blind spots and IT strain

In addition to planning ways to support efficient clinical workflows in shared mobile device environments, IT teams must also plan ways to streamline operations to maximize their ROI. For example, **75%** of respondents say care team members frequently have to contact the help desk to remediate being locked out of mobile devices or applications, thereby increasing costs and adding strain to already over-burdened IT teams. As help desk tickets cost an average of $70 each, a shared mobile strategy that minimizes help desk calls by streamlining authentication and access processes results in considerable cost savings.

Other device management challenges for IT teams include lack of visibility into mobile device usage, lack of a centralized system for managing mobile devices, time-consuming setup processes, and a lack of a reliable way to track mobile devices.



When it comes to IT teams' lack of visibility into mobile device usage:

48% lack visibility into which users were assigned a device

53% lack visibility into when devices were last assigned

55% lack visibility into what applications are being accessed

As a result of inconsistent, manual, and/or non-existent shared-use mobile device policies, IT teams are spending a significant — and unnecessary – amount of time managing their shared-use devices. **On average, they dedicate 32% of their time to maintenance, 25% to tracking, and another 25% to monitoring these devices.**

These blows to efficiency point to a deeper need: nearly all IT decision-makers **(95%)** believe their care facility could improve how it controls user access to applications and data on shared-use devices. And just as many **(95%)** say the same about their ability to audit device status and usage.

> **“Imprivata has greatly improved access to systems and enhanced staff workflows. There is reduced login friction and fewer support tickets for IT to deal with regarding password resets. As an organization we have more visibility of device usage and more accurate real-time reporting.”**
>
> – Grant Morris, ICT Project Manager, Sundale Ltd

Security and accountability risks

An informal or inconsistent approach to shared device assignment creates workflow issues and a lack of accountability, while also increasing security and privacy risks. Unfortunately, **16%** of respondents say that they have no consistent policy or process in place for assigning devices at the start of each shift. **Forty-six percent** of organizations use verbal or other informal processes for assigning devices, and **28%** use a “first come, first served” method where staff members pick up any available device with no documented checkout or assignment process.

> **“We’ve had instances where it’s unclear whether someone has logged out properly after using the mobile devices. It’s a bit of a grey area, and sometimes we’re not sure which staff member last accessed sensitive data.”**
>
> – IT decision maker, 750-999 bed facility, U.S.

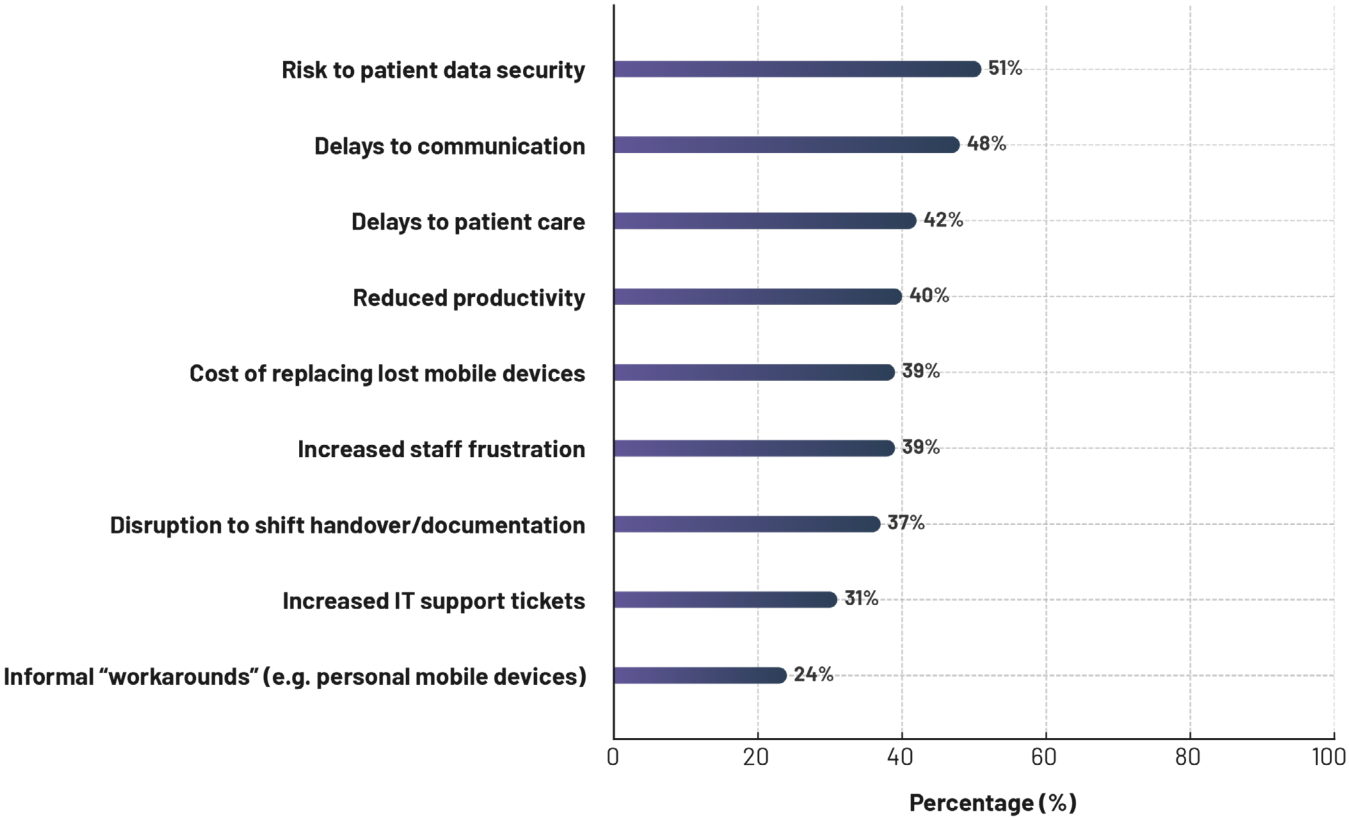
The most common challenge organizations face when it comes to shared-use mobile devices is concern around data security, as cited by **44%** of respondents. Risk is exacerbated by the user access workflow and IT operational challenges highlighted earlier. For example, **79%** of respondents say employees within their organization share credentials when accessing shared-use devices. Furthermore, **74%** of respondents say shared-use devices are frequently left signed in by staff after use, potentially exposing personal health information (PHI) or other sensitive data. These problems are likely why **49%** of respondents are not completely confident that patient data is fully protected on their shared-use mobile devices.

The most common challenge organizations face when it comes to shared-use mobile devices is concern around data security, as cited by 44% of respondents.

The costs of device loss

Another costly challenge is the number of shared-use mobile devices that are lost, stolen, or otherwise missing. **Twenty-three percent** of shared-use mobile devices are lost annually, and the high cost of loss comes from more than just the price of replacing devices. When a device is identified as missing, organizations experience average care team delays of three hours per week per device, with **26% of organizations saying that it may take a full working shift (up to 12 hours) to locate a missing device.**

What impact do missing, misplaced, or unavailable shared-use mobile devices have on your care team?



“With our old system, about 20% of our devices went missing every year, but Imprivata Mobile Access Management makes it easy for us to track check-ins and check-outs. It helps us improve accountability and a significant contributing factor in yielding annual savings of approximately $500,000 a year in expenses related to device loss.”

– Michael Paulemon, DTS Manager, Workplace Technology & Engineering, Yale New Haven Health

> **“Shared-use mobile devices may be at risk of unauthorized access. Since multiple staff use them, ensuring data privacy compliance like HIPAA is challenging. Also, if devices are lost or stolen, sensitive patient data could be exposed.”**
>
> – Clinical leadership, 500-749 beds, U.S.

High rates of device loss can be attributed, in part, to outdated tracking methods, with around a third of respondents saying their facility still relies on manual sign-out sheets **(36%)** or Microsoft Excel **(32%)** to track device locations.

> **One limitation ... is the lack of real-time tracking for device usage, which makes it challenging to monitor where devices are and whether they are being used properly.”**
>
> – IT decision maker, 500–749 bed facility, U.S.

Unlocking the full value of shared devices

Shared-use mobile devices offer tremendous promise — but only when managed with the right policies, workflows, and technology. This report reveals that:

- The ROI is real — but strategy has a big impact
- Solutions that optimize workflows also improve clinical productivity and patient throughout
- IT burden and data security risks must be addressed
- Identity-driven, policy-enforced management is essential

Remember, facilities that implement comprehensive shared mobile access management solutions can yield a **63% greater ROI** than facilities with fragmented or informal approaches to shared-use mobile devices. Better access management solutions also help mitigate risks associated with device loss and data breaches.

Now is the moment for healthcare organizations to harness the full potential of shared mobile technology. By investing in purpose-built technologies and implementing policies and processes that address the unique needs of shared mobile programs, healthcare organizations can maximize the considerable clinical and operational value of shared-use mobile devices.

Methodology

- **Regions:** U.S., Canada, U.K., Australia
- **Respondents:** 242 IT decision-makers, and 158 clinical leaders
- **Facility Sizes:** 100–1,000+ beds

Approximately how many patient beds does your hospital have in total? Average number of beds

	Data Split: Total	
	Total	
	Count	%
Total	*400*	*400*
100-249 beds	39	10%
250-499 beds	104	26%
500-749 beds	92	23%
750-999 beds	85	21%
1,000 or more beds	80	20%
Mean	669	669

Respondent Type								
	Data Split: Total		**Data Split: Country**					
	Total		US and Canada		UK		Australia	
	Count	%	Count	%	Count	%	Count	%
Total	*400*	*400*	*200*	*200*	*125*	*125*	*75*	*75*
IT decision maker	242	61%	121	61%	77	62%	44	59%
Clinical leadership	158	40%	79	40%	48	38%	31	41%

Country distribution for respondents overall:

- 140 – U.S.
- 60 – Canada
- 125 – UK
- 75 – Australia

imprivata®

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 organizations 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

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533