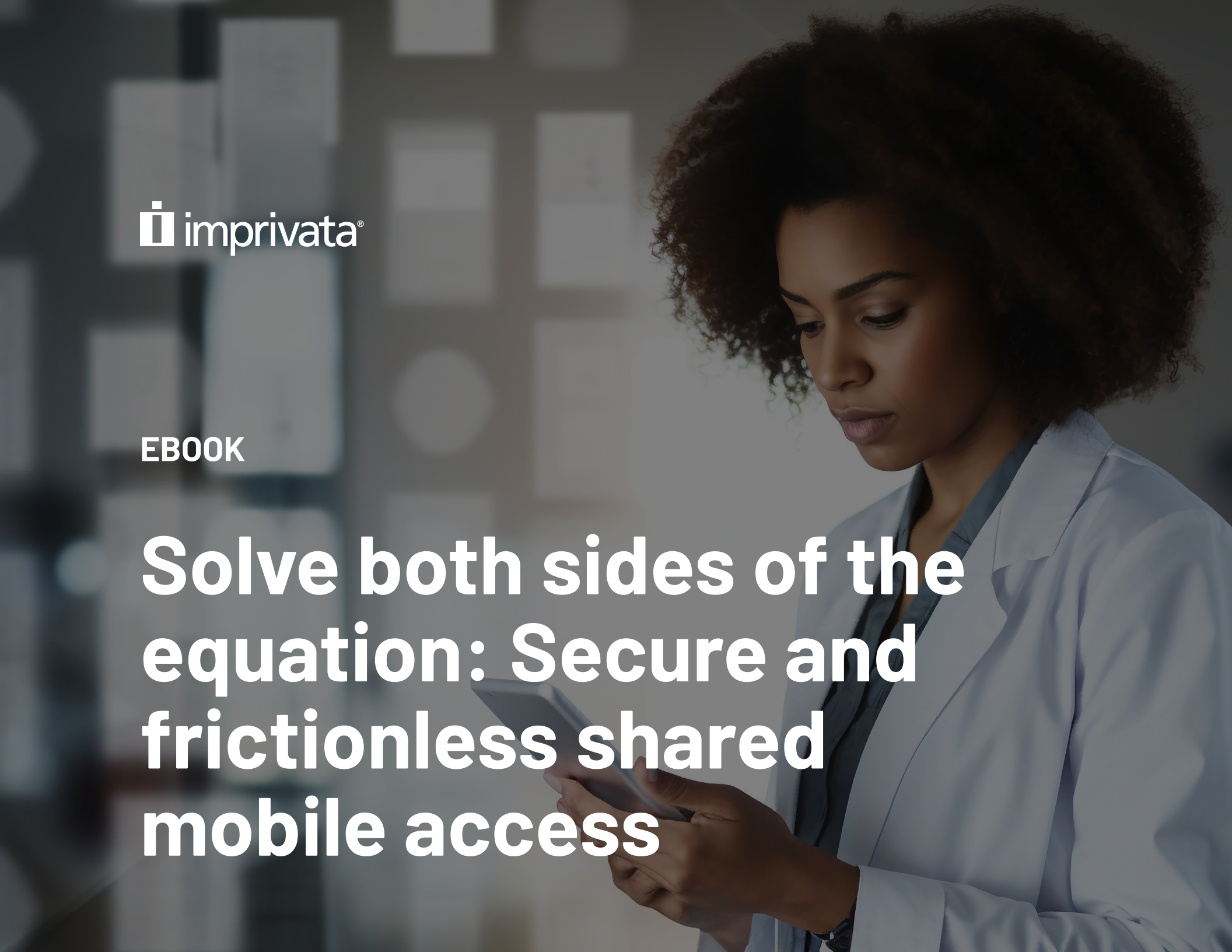

imprivata®

EBOOK

Solve both sides of the equation: Secure and frictionless shared mobile access

Let's face it. Crafting, implementing, and gaining buy-in for a mobile strategy in healthcare environments is difficult, particularly with the many security, privacy, and compliance requirements involved.

But mobile workflows are the present – and future – of healthcare. With efficient and secure mobile workflows, organizations have the freedom and flexibility to deliver enhanced 24/7 care while maximizing IT investments. Resource challenges become a little less challenging when clinicians have access to information whenever and wherever it's needed.

Bottom line: striking a careful balance between strong security and clinician convenience is crucial.

Starting with shared devices

For healthcare organizations, a shared-device strategy tends to be the most cost-effective approach to mobile. A shared environment also supports nursing workflows, reduces distractions, and makes it easier to maintain the device environment while enforcing security and access control.

Despite the many benefits, every door that mobile use opens is a potential point of entry for bad actors, data breaches, and other security issues. And managing a fleet of devices to optimize technology investments and prevent device loss can be a major challenge. Plus, adoption can be a big hurdle – you can't benefit from the improved care delivery and efficiency promised by mobile technology if clinicians don't use the devices.

So how do you make mobile technology truly work for your organization and your people? How exactly do you safeguard privacy and security without hampering efficiency?

A shared environment supports nursing workflows, reduces distractions, and makes it easier to maintain the device environment while enforcing security and access control.

Take a closer look at what's happening

To understand and overcome the challenges of mobile technology, it helps to begin by examining the experiences and needs of the people meant to use the devices.

Healthcare workers perform tough, high-stakes jobs that are seeing unprecedented rates of burnout, with many leaving the profession. One study predicts that the United States will lose more than **6.5 million healthcare professionals by 2026,** with only 1.9 million workers on track to replace them. A 2023 workforce plan produced by England's National Health Service (NHS) states that they are **currently short of 154,000 full-time workers.** If trends continue, that figure could balloon to 571,000 by 2036.

What's behind the burnout?

One prominent reason for clinical burnout is the considerable administrative burden of healthcare. Evaluating and recording notes for an endless line of patients, hours spent maintaining EHR/EMR records, and constantly facing the challenges of complicated technologies that require up to 70 logins per shift is a daunting list.

You can't counteract burnout if you're simultaneously adding to it with inefficient workflows and security approaches that create barriers to clinician productivity.

A strong shared mobile environment can help lighten this burden considerably, going a long way to counteract burnout. For example, mobile devices can enable clinicians to chart at a patient's bedside, in real time, without dragging around a clunky workstation.

Still, though, you can't counteract burnout if you're simultaneously adding to it with inefficient workflows and security approaches that create barriers to clinician productivity.

Take, for example, the struggle to remember which complex, 16+ character password goes with which application. The struggle itself creates cognitive distraction that interferes with quality patient care, and even the best medical tools in the world are useless if you can't quickly access them when needed. The resulting delays and frustrations can also lead to security issues due to workarounds. Clinicians focus on immediate patient care, and they're inclined to take risks like sharing passwords if it allows them to promptly respond to patient needs.

If you want your mobile technology to be adopted and used securely – it needs to be purpose-built, with clinician input, to seamlessly integrate into workflows.

So, what's the answer?

Driving the adoption and useability of shared mobile devices requires user access management tools that offer a personalized end user experience without compromising security. That includes:

- Creating a secure, personalized device environment without repetitive, manual workflows
- Achieving a fast, intuitive access to the best device, every time
- Adding convenience for device checkout with a simple badge tap
- Streamlining access to critical applications by eliminating repetitive, manual authentications, and other efficiency road bumps
- Protecting data and privacy by locking down devices between each use, and maintaining control over who has access to what, when
- De-personalizing devices after use with less time and effort, and without burdening end users, further supporting privacy and device readiness

CONTINUE READING >