LINQ

Security, Simplicity, and Savings:

The Case for Enterprise Mobile Management in Healthcare

LINQ

Table of Contents

Healthcare is an ever-evolving space that must pivot, adapt, and grow to meet the growing demands of patient populations, and ensure quality care. Because doctors, practitioners and other professionals working in this industry need instantaneous access to personal medical information at the point of care, mobile devices have emerged as fast, effective, and reliable tools to facilitate day-to-day workflows.

Between 2017 and 2022, mobile device usage increased from:

- **65% to 97% among bedside nurses**
- **51% to 98% among physicians**

Mobile devices increase efficiencies, enhance collaboration, and improve patient outcomes. For instance, nurse managers say clinical mobility reduces medication errors, patient care issues, and preventable medical errors, which are more likely to occur amid poor communication.

Furthermore, clinicians use mobile devices to access electronic health records, perform bedside documentation, and collaborate with colleagues. Mobile devices also support popular advances such as telehealth and remote patient monitoring. Patients report higher satisfaction, too, when healthcare providers incorporate mobile devices into their care.

There is no doubt that mobile devices are essential to modern healthcare. Yet they can be complex to manage — requiring ongoing maintenance and cybersecurity protocols to ensure strict compliance and protect patient privacy. In this ebook, we'll unpack why it's advantageous for healthcare organizations to partner with a managed mobility services provider who can play a key role in leveraging the efficiencies of mobile devices without burdening IT staff, incurring unnecessary costs, or risking confidential data.

Improving Compliance Through Centralized Mobile Device Management

Every gateway to a healthcare computing system, whether that be a mobile phone, tablet, or laptop, is a vulnerability that could expose sensitive health information to the wrong people. That's why compliance with HIPAA and other government regulations is a key priority for healthcare providers.

If mobile devices are not adequately protected, they have the potential to breach compliance as they connect to the network, and as employees use their devices to access sensitive information. This can result in hefty fines, reputation damage, and even patient endangerment.

Enterprise mobility management minimizes the risk of non-compliance by ensuring that mobile devices are equipped with the proper security protections. That includes ongoing software updates and patches that defend against emerging security threats.

Mobility management also supports compliance by centralizing control over employee mobile devices. Healthcare providers must impose consistent parameters over what employees can do with their mobile devices and the type of information they can access. Installing mobile device management (MDM) tools to force passcodes, encrypt data, and limit data leakage can help reduce security risks.

Often in-house IT administrators are tasked with handling mobility management, including MDM, but this only adds to the complexity that in-house IT teams must navigate. As an alternative, healthcare organizations are finding it more efficient and cost-effective to work with a managed mobility services provider that specializes in MDM. This partnership mitigates the need to add headcount to in-house teams, while also supplying the MDM experience that keeps devices safe and connected.

$1.5 million

The potential fine for failing to correct HIPAA violations

Common Security Threats and Scams Targeting Mobile Devices

Digitizing medical workflows has enormous advantages, but it also creates risk. As healthcare organizations increase their use of mobile devices, they must take additional precautions to keep patient and organizational data safe. Mobile device security is critical for two reasons. First, mobile devices are a popular target of attacks. Second, healthcare organizations are a favorite target of cybercriminals (we'll explore why in the next section).

Phishing is among the most common types of attack particularly targeting the healthcare industry. Phishing essentially takes advantage of users by masquerading as a trusted or recognized source.

11 years

The number of consecutive years that the healthcare industry has had the highest average costs of a data breach — on average, **$9.23 million** in 2021

While phishing schemes typically rely on email, attachments, and webpages to capture private data, social engineering is another type of attack that might use these, the phone, or any number of different methods to psychologically manipulate victims into handing over personal information. Beyond that, "watering hole" attacks are also becoming increasingly common, especially on mobile devices. These attacks rely on users to connect to unsecured public Wi-Fi networks at their go-to lunch or coffee spot. Hackers intercept these unsecure networks and gain access to private information.

"The most daunting challenge remains IT security/cybersecurity. A malware attack remains the most likely reason for an acute and widespread interruption of business in the healthcare space. A successful malware attack has damaging long-term effects to reputation, infrastructure, and team morale as well. The challenge here is that our patients and workforce want more access, which makes it more difficult to secure the business."

David Seo, CIO, Nicklaus Children's Health System
Source: WittKiefer, 2022

The top causes of data breaches in 2021 potentially involving mobile devices:

- Social engineering
- Phishing
- Compromised email
- Compromised credentials
- Accidental data loss or lost device

Why Healthcare Remains a Prime Target for Cyber Criminals

Today every organization is vulnerable to security threats, but healthcare organizations are a prime target.

Protected health information (PHI) is more valuable to hackers than other types of stolen information because it fetches a higher price on the dark web. PHI may include several different types of personal data, from Social Security numbers to biometric identifiers. It is also less likely to be modified than other types of stolen information, such as credit cards.

Fierce Healthcare notes that in addition to using PHI to accomplish financial fraud, such as creating false identities to open loans and credit card accounts, criminals can also use PHI to obtain illegal prescriptions and file fraudulent medical claims.

As a result, PHI is one of the most lucrative types of data that hackers are looking for in a ransomware attack or a stealthy data theft. Such incidents are incredibly costly for healthcare providers. Victims of ransomware and data theft may spend millions of dollars to address the financial, legal, technological, and reputational fallout of a breach.

$250–$1,000

The value of a medical record on the dark web, compared to $4 for a Social Security number

41%

The percentage of security leaders who cite increased use of managed security services partners/ outsourcers as a promising security strategy

According to U.S. government data, the number of healthcare breaches in the first five months of 2022 has nearly doubled from the same period last year.

How Enterprise Mobile Management Reduces Security Risks

Modern security threats mean that the more reliant healthcare providers become on mobile devices, the more defenses they must put in place. Using MDM tools and other solutions, healthcare organizations can strengthen their defenses by:

- Consistently keeping devices and software up to date
- Ensuring that company security policies are deployed consistently across the organization
- Separating company apps from personal apps
- Controlling what employees can and cannot access on their devices
- Remotely locking and wiping lost or stolen devices
- Assist with data leakage prevention

Ongoing Workforce Shortages Highlight the Need for an Expert Partner

Staffing shortages — pre-dating the pandemic but severely worsened in its wake — are a critical challenge across the healthcare industry, including registered nurses, technicians, therapists, physicians, and specialists. It's also important to note that many organizations are struggling to hire qualified IT and cybersecurity staff as demand for technology jobs across all sectors outweighs the number of people available to work.

The tech talent shortage is actually expected to get worse before it gets better, with a recent survey by TalentLMS and Workable, showing that a sweeping 72% of employees working in tech/IT roles are thinking of quitting their job in the next 12 months. This is significantly higher than a 55% rate of the overall U.S. workforce. Furthermore, another survey from ResumeBuilder.com showed that 18% of tech/IT employees in healthcare plan to quit in 2022.

Numbers like these make it clear that healthcare organizations must do everything they can to reduce the burden on existing personnel. Mobile management helps address that goal by handling all the back-end support and maintenance that allows for high-quality connectivity, mobile workflows, and reduced cybersecurity risks.

"There are many challenges facing CIOs today, but the top of the list is definitely finding and retaining talent. The Great Resignation has affected healthcare IT as well."

Carmella Cassetta, CIO and Vice President of Hoag Memorial Hospital Presbyterian, Newport Beach, California
Source: Becker's Hospital Review, 2022

How Enterprise Mobile Management Supports Doing More with Less

Instead of spending precious staff resources managing mobile devices and plans, healthcare organizations can transfer all that work to a managed mobility services provider that will:

- Manage onboarding and offboarding staff mobile devices
- Provision and troubleshoot employees' devices
- Keep devices updated with the appropriate software and applications
- Monitor and manage data usage to ensure employees have the connectivity they need in the most cost-effective manner
- Provide a single point of contact by dealing with carriers on providers' behalf
- Take charge of mobile asset recovery and disposal as well as inventory management

That frees medical personnel and administrative staff to focus on more critical tasks, including caring for patients.

Mobility Partners Offer Expertise to Reduce Device Costs

Staffing may be the biggest concern for healthcare organizations, but financial challenges are a close second, according to the American College of Healthcare Executives. Billions of dollars of lost revenue during the pandemic, rising drug prices, and increases in labor and supply costs have pushed many providers into a financial crisis.

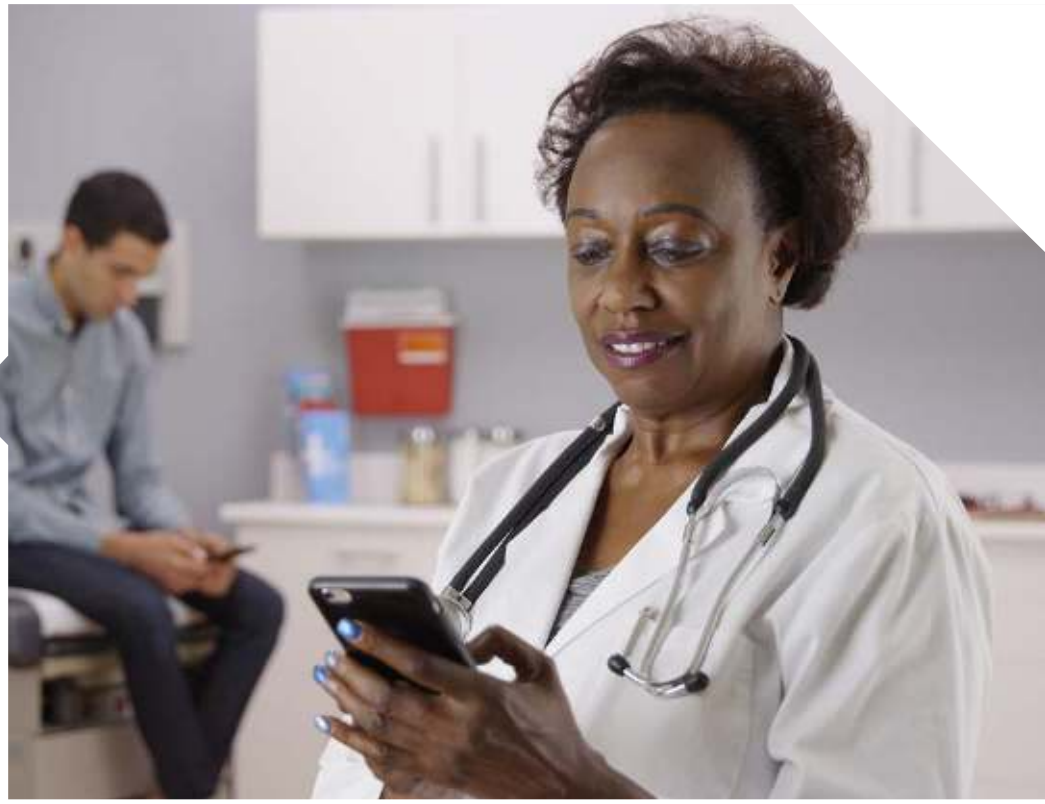
While technology strategies are only one piece of a complex puzzle, partnering with experts is one way to control costs associated with essential workplace tools, such as mobile devices. Healthcare providers can experience direct savings as well as many other benefits with a managed mobility services partner who can assume the following tasks that often take up time, money, and resources, including:

- Working on providers' behalf to dispute and resolve billing issues
- Negotiating better rates for mobile devices and data plans
- Taking advantage of economies of scale
- Analyzing device and data usage to understand trends and identify cost-savings opportunities

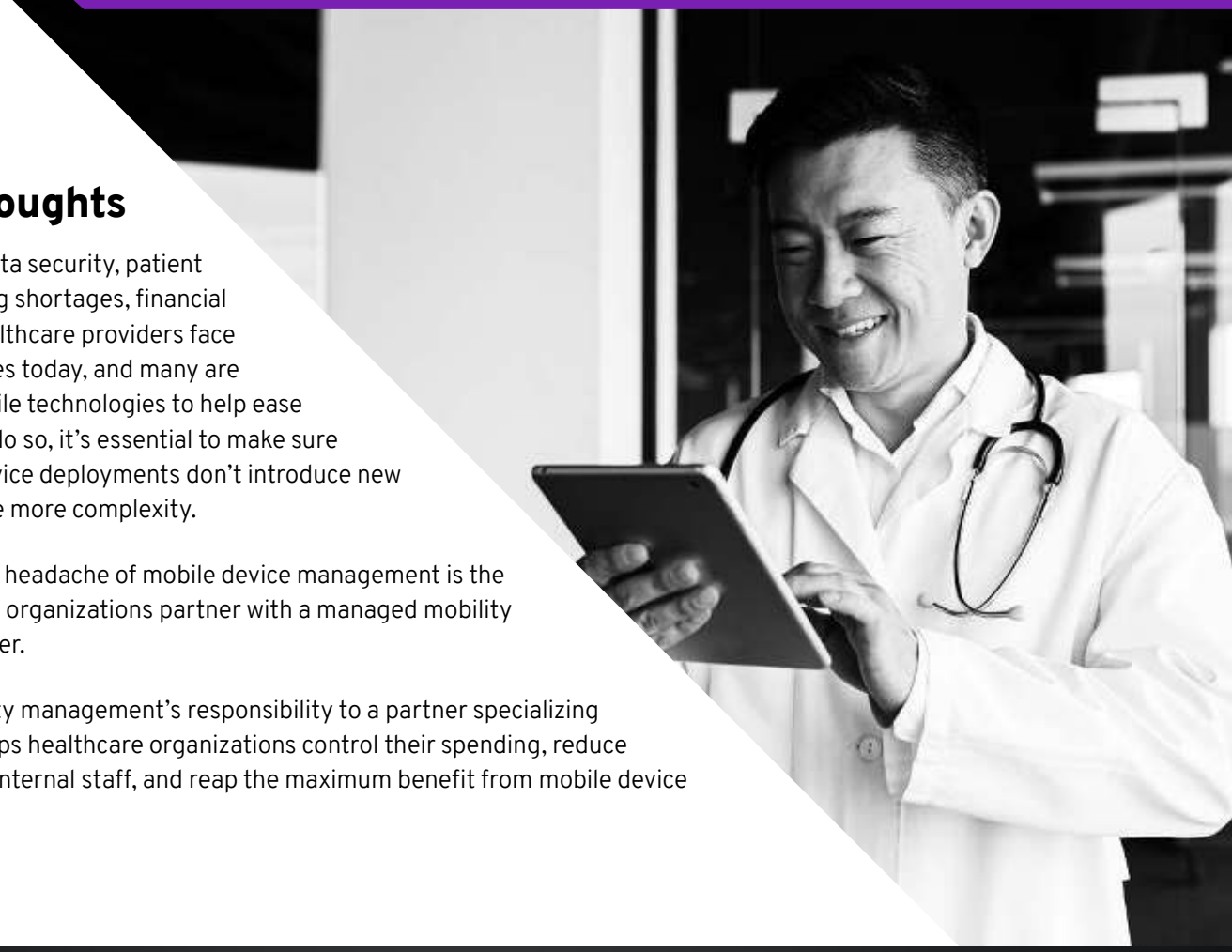
20%

Unmanaged direct mobility costs can be 20% greater compared to a managed environment

Between helpdesk, email, security and invoice management, enterprises devote two-to-three full-time equivalents for every 1,000 mobile devices.



"Most of the nation's hospitals were operating on razor-thin margins prior to the pandemic; and now, many of these hospitals are in an even more precarious financial situation." **American Hospital Association, 2022**



Final Thoughts

Compliance, data security, patient privacy, staffing shortages, financial concerns — healthcare providers face many challenges today, and many are looking to mobile technologies to help ease them. As they do so, it's essential to make sure that mobile device deployments don't introduce new issues or create more complexity.

Simplifying the headache of mobile device management is the primary reason organizations partner with a managed mobility services provider.

Shifting mobility management's responsibility to a partner specializing in this work helps healthcare organizations control their spending, reduce the burden on internal staff, and reap the maximum benefit from mobile device investments.

LINQ

Reach out to learn more about how LINQ can save time and money and your company's cellular services.

Ask about our 60-day free trial.

BALTIMORE
101 W. Dickman Street
Suite 400
Baltimore, MD 21230

PITTSBURGH
125 7th Street
Floor 6
Pittsburgh, PA 15222

LAS VEGAS
9075 W. Diablo Drive
Suite 120
Las Vegas, NV 89148

INFO@LINQSERVICES.COM • 800-421-5467

WWW.LINQSERVICES.COM