WEIGHING THE TOTAL COSTS AND BENEFITS OF OWNERSHIP

Healthcare Enterprise Mobility Solutions vs Consumer Devices

Honeywell

TABLE OF CONTENTS

INTRODUCTION

Healthcare mobile devices are the mainstay of the clinician, staff, and patient interaction in hospitals, clinics and other healthcare workplaces. Healthcare providers use this technology to access information quickly from anywhere and stay connected to patients and to one another, which drives efficiencies and improves the speed and quality of patient care.

The healthcare environment demands the highest level of efficiency, speed, durability and security. When healthcare workers have all the data they need in the palm of their hands, they can spend less time on administrative tasks and more time caring for patients. Mobile devices are used for[1]:

- **Information management.** Note-taking, audio recording, photography, ebook access and cloud services.
- **Time management.** Appointments, meetings, call recordings.
- **Health record maintenance.** Access to electronic records, acc to scans/x-rays, electronic prescribing, billing.
- **Communications.** Voice and video calling, messaging, email, video conferencing, social networking.
- **Reference.** Medical literature, search portals, drug reference guides, medical news.
- **Patient monitoring.** Rehab assessment, heart monitoring, clinical data collection.
- **Medical education & training.** Continuous assessment, board exam preparation, case studies, elearning, surgical simulation.

With hundreds of thousands of mobile devices now requiring access to a healthcare network, it is no surprise that mobile data security and HIPAA compliance have become two of the biggest concerns for CIOs, CISOs, Compliance Officers and Healthcare IT professionals.[1] Healthcare workers need a secure mobility solution they can take with them anywhere, which can be updated on the spot. That device must interface succinctly with point-of-care delivery, documentation and identification functions seamlessly.

1. The Use of Mobile Devices in Healthcare - https://www.psqh.com/analysis/the-use-of-mobile-devices-in-healthcare/

When considering mobile devices' acquisition for Healthcare, there are three kinds of mobility solutions organizations consider: Consumer Devices, Healthcare Enterprise Devices and Bring Your Own Device (BYOD).

Often the discussion centers around whether to purchase consumer vs. healthcare enterprise mobile devices. Choosing a suitable device for your healthcare environment comes from evaluating a variety of quantifiable variables. The result is a mobile deployment that can increase workforce/workflow productivity, task accuracy, and measurable return on investment (ROI).

As VDC Research explains, not all mobile solutions are equal. "Failing to align the 'right' mobile solutions with the target application or use case can expose organizations to significantly higher cost of ownership. This places apremium on reliability for business-critical solutions to minimize the disruptiveimpact of solution failure and visibility to quickly identify and respond to problems that do arise."[1]

This whitepaper will review some of the essential differences between consumer and healthcare enterprise mobile devices and their total cost of ownership (TCO).

1. VDC Research Group, Inc. | Enterprise Mobility, "Total Cost of Ownership Models for Line of Business Mobile Solutions," December 2018

WHY HEALTHCARE NEEDS ENTERPRISE MOBILE DEVICE SECURITY

1

Healthcare providers increasingly use mobile devices to store, process and transmit patient information. This information is especially vulnerable to attack. When health information is stolen, inappropriately made public, or altered, healthcare organizations can face penalties and lose consumer trust, and patient care and safety may be compromised.[1]

In a HIMSS-Honeywell survey, 94% of respondents listed security and compliance as the most important factor when considering vendors.

According to the US Departing of Health and Human Services[2], anyone with physical access to such devices and media, including malicious actors, potentially has the ability to change configurations, install malicious programs, change information, or access sensitive information. Any of these actions have the potential to adversely affect the confidentiality, integrity, or availability of protected health information (PHI).

MOBILE DEVICES ARE A POTENTIAL MINEFIELD OF HIPAA VIOLATIONS

While improved productivity and the clinician experience are often stated as the main reasons for implementing a mobile communications solution, security and HIPAA compliance are top priorities when vetting providers.[3] In a HIMSS-Honeywell survey, 94% of respondents listed security and compliance as the most important factor when considering vendors.[4]

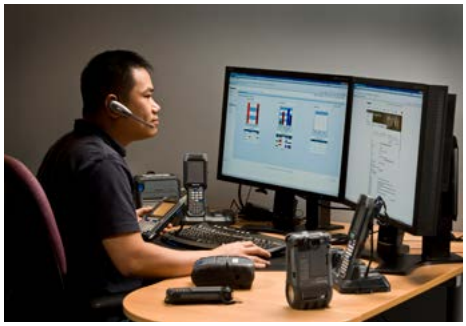
Even with secure mobile devices, there is substantial potential for users to violate HIPPA rules or company policies. Without the necessary controls, devices can be compromised, and the electronic Protected Health Information (ePHI) stored on them exposed. Consumer-grade mobile devices (i.e., smartphones, tablets, and laptops) are the target of cybercriminals because they are viewed as easy entry points into the healthcare network.

The issue goes beyond HIPAA requirements. PHI, medical devices and other data are vulnerable to cyberattacks due to both outdated clinical technology and the use of consumer-grade devices. These devices often lack robust security controls, used to connect to networks via public Wi-Fi, and there is considerable potential for theft or loss.[5]

Many hidden expenses must be considered, such as reputational damage, customer turnover, and operational costs. Knowing where the costs lie and how to reduce them can help companies invest their resources more strategically and lower the huge financial risks at stake.[6]

1. National Institute of Standards and Technology (NIST) and the National Cybersecurity Center of Excellence guide, Securing Electronic Records on Mobile Devices - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-1.pdf
2. US Departing of Health and Human Services: Office of Civil Rights1 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-1.pdf
3. Honeywell. 2020. Shutting down mobile technology security risks in Healthcare [infographic] - https://now.honeywellaidc.com/rs/801-ATQ-538/images/Honeywell%20Mobile%20Security%20Risks%20Infographic_06.17.20.pdf
4. HIMSS-Honeywell survey
5. Mobile Data Security and HIPAA Compliance https://www.hipaajournal.com/mobile-data-security-and-hipaa-compliance/
6. The Use of Mobile Devices in Healthcare https://www.psqh.com/analysis/the-use-of-mobile-devices-in-healthcare/

HEALTHCARE DATA BREACHES ARE THE COSTLIEST



According to IBM Security's 2020 report, healthcare data breaches are the costliest. The cost of an average healthcare data breach is $7.13 million globally, with an average cost of $146 per record. In the United States, the average cost for a breach was $8.6 million or $175 per record. To put it in perspective, a breach of 1 million to 10 million records cost an average of $50 million, breaches of 10 million to 20 million records cost an average of $176 million, and a breach of 50 million records was calculated to cost $392 million to resolve.[1]

Globally it took 280 days to detect and contain a breach and 315 days to detect and contain a malicious attack. In the United States, it took an average of 186 days to identify a data breach and 51 days to contain the attack.[1]

ENTERPRISE MOBILITY SOLUTIONS ARE REQUIRED

It is common for IT to manage a portfolio of mobile healthcare devices across multiple facilities, associations, professional groups and departments. Because of all the distinct networks, managing IT issues centrally and sharing protected health information (PHI) is challenging. You need a mobility solution with advanced security.

When you choose a healthcare enterprise device, you gain an enterprise mobility solutions platform and a complement of features that protect the healthcare data you simply don't receive with a consumer-grade device.

HOW HONEYWELL STRENGTHENS ENTERPRISE DEVICE SECURITY

Honeywell has a deep institutional and cultural focus on security across multiple domains. Across Honeywell, we invest over $50 million annually in cybersecurity and employ 300+ dedicated security professionals focused on protecting our customers.

We design security into our products, policies, and processes. The best way to ensure that you have a secure device is to make sure you use the most recent version of the operating system and up-to-date security patches. We provide a regular security patch cadence for Mobility Edge devices of at least every 90 days and often as frequently as every 30 days. OS version upgrades are provided annually.

Our security built-in, design-to-delivery process strongly emphasizes programming security into products to anticipate and mitigate risk. We do this by embedding deep domain knowledge of industry-leading security practices throughout our entire design and development process to ensure our solutions are as secure as possible from the start. We also make our solutions as free of vulnerabilities to attack as possible through such measures as continuous testing, authentication safeguards, and adherence to best programming practices. And, this isn't anything new for Honeywell. We have had over 1,000 global engagements since 2006 and are the provider of managed security services for over 350 industrial sites. To continue our focus and lead the way in the industry, we put in place the industry's first Cybersecurity Risk Manager and developed strategic partnerships with leading cybersecurity product vendors.

1. IBM Security 2020 Cost of Data Breach Report Shows 10% Annual Increase in Healthcare Data Breach Costs - https://www.hipaajournal.com/ibm-security-2020-cost-of-data-breach-report-shows-10-annual-increase-in-healthcare-data-breach-costs/

HEALTHCARE ENTERPRISE MOBILE DEVICES ARE PURPOSE BUILT

2

When evaluating mobile devices for your healthcare staff, there are many factors to consider. Selecting the wrong device can frustrate users, decrease productivity, increase costs, and cause safety risks. When choosing the correct device, you can maximize workforce productivity, task accuracy and a higher return on investment (ROI).

For a mobile solution to meet all clinicians' needs, the device must work 24/7. Dropped calls and taking a device out of commission for repairs or recharge a battery can lead to delays, costly mistakes and miscommunication. All of these scenarios frustrate clinicians and affect patient care.

On the surface, consumer-grade devices can appear like the best choice for reasons such as:

- Healthcare staff are familiar with how the devices work.
- The devices have a small form factor making them easy to carry.
- The upfront cost of the consumer-grade device is considered inexpensive.

Consumer-grade devices are designed for single-user, slow-moving applications like texting, making phone calls, and accessing social media, music, movies and games. When you put those devices into healthcare environment workflows, the consumer-grade devices must be able to withstand enterprise-level performance standards such as security, drops, bumps, tosses, extreme heat and cold, multiple users, exposure to hospital-grade cleaners and more.

The disadvantages of the consumer-grade devices are revealed when compared to healthcare enterprise devices specifically designed for the healthcare environment. These differences should be carefully evaluated by hospital decision-makers when selecting the suitable, best-in-class device to help improve staff productivity, communication and enhance the patient experience. Let's consider just a few of those differences.

Honeywell believes that customers invest in solutions, not devices. Toward that end, we work with our healthcare customers to understand the business objectives and assemble complete solutions to solve those problems. This not only means building innovative and powerful computers but also includes:

- Purpose-built industrial design that optimizes user experience
- Accessory systems that are optimized for the use case, easy to use, with forward and backward compatibility
- Platform software that provides continuous and robust compatibility, security and support for the life of the product
- Honeywell deployment tools that accelerate time-to-value
- Relationships with independent software providers that provide critical apps to complete customer solution sets

PLATFORM DESIGN

Honeywell believes that customers invest in solutions, not devices. Toward that end, we work with our healthcare customers to understand the business objectives and assemble complete solutions to solve those problems. This not only means building innovative and powerful computers but also includes:

- Purpose-built industrial design that optimizes the user experience.
- Accessory systems that are optimized for the use case, easy to use, with forward and backward compatibility.
- Platform software that provides continuous and robust compatibility, security and support for the life of the product.
- Honeywell deployment tools that accelerate time-to-value.
- Relationships with independent software providers that provide critical apps to complete customer solution sets.

Honeywell recognized that industries like Healthcare wanted a unified hardware and software platform for all form factors – one that allowed for rapid deployments, robust performance, and adaptability to changing needs. We completely innovated our approach to meeting the challenges of supporting a mobile workforce, and Mobility Edge was the answer.

Honeywell's Mobility Edge™ delivers an innovative solution to these challenges.
Mobility Edge offers an integrated, repeatable, scalable approach to device management that is based on a common hardware and software platform. Designed for Android it delivers a unified platform on which all software solutions are based. Healthcare can develop and deploy faster while reducing development costs.

By providing a unified hardware and software platform with an agile approach, we can bring you more secure and reliable solutions across your operation.

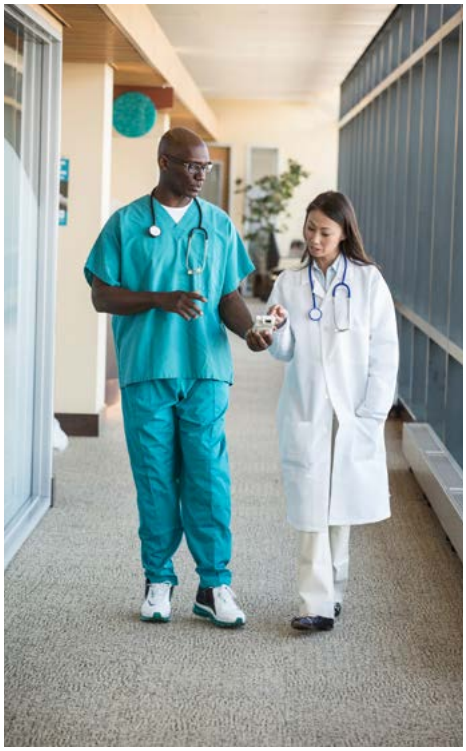
The common platform provides for the efficient reuse of IT investment across multiple form factors both across the present fleet and over the future roadmap. It is accompanied by a common deployment toolset that speeds time-to-value and the Operational Intelligence cloud optimization and management platform that provides visibility into device location, condition and full-life maintenance history. All of the devices are supported by popular MDM solutions as well.

THINK ANDROID PLATFORM FIRST, ENTERPRISE DEVICE SECOND

When choosing a mobile device for Healthcare, one of the critical considerations is the operating system (OS). In Healthcare, this decision usually comes down to iOS vs. Android.

When hospital chooses iOS, they commit to an OS and a one set of hardware (iPhone, iPad, and iPod Touch). With the Android OS, the hospital is now open to hundreds of more options.

All enterprise devices running on Android are not the same. Honeywell has been working with Android since 2011. We have made massive investments in Android engineering competency. Honeywell helps companies confidently select, deploy, and manage Android operating system devices and services. As part of the Google-led Android Enterprise Recommended Managed Service Provider program, Honeywell provides customers more confidence in deploying Android solutions and ensuring their enterprise mobility deployment is consistent and current.



Honeywell provides customers with a comprehensive set of enterprise services that address every mobility lifecycle phase to help streamline operations and reduce IT-related costs. Honeywell globally manages more than two million devices such as purpose-build enterprise smartphones, tablets, and mobile computers. Honeywell has a community of hundreds of softwarepartners and works with key industry leaders to ensure devices are certified and validated for regulatory compliance and seamless integration.

HEALTHCARE UNIFIED COMMUNICATIONS

Whether you need a push-to-talk feature for nurses or the ability to take a call from the PBX, healthcare workers need a device that provides excellent voice and video calling, messaging, email, video conferencing 100% of the time.

A consumer device doesn't offer the secure, enhanced worker communication needed in Healthcare. Consumer devices are not configured for highly dense buildings and remote areas. This can be the cause of dropped calls, poor voice and video quality during patient care.

Honeywell provides an all-in-one mobile device communication solution with Honeywell Smart Talk for Healthcare Communications. Honeywell Smart Talk is a true voice-enabled unified workforce communications application for healthcare organizations that tackles fragmented communications. You receive enterprise-grade security for voice calling, text and media messaging, and user presence. Smart Talk can be added to Honeywell CT40 HC Mobile Computer or most types of mobile devices associates already carry.

You enable smarter communications for the entire hospital operations team from a single mobile device. One device to manage and maintain. One device replacing the need to support and buy consumer mobile phones. With a constant and instant connection, the enabled device allows hospital staff to have the tools and information they need to deliver an exceptional patient care experience.

DURABILITY AND EASE OF USE

A typical consumer may drop their phone at home or spill a few drops of coffee on it. That's nothing compared to a healthcare environment. A clinician may drop the device frequently on hard concrete floors. During 24 hours, multiple people may touch and use the device.

Enterprise-level devices tailored to the healthcare setting are encased in an enterprise-level healthcare-grade protective housing. While tough casing protects against hardware failure, internal components also influence a product's lifecycle. In the healthcare environment, with its increased focus on delivering higher quality care at a lower cost, a longer lifecycle can lead to significant cost savings – a measurable return on investment.

Honeywell enterprise device computers combine the advantages of consumer devices and the purpose-built enterprise computers into a single package. Like consumer devices, Honeywell devices are designed with the user in mind, and they provide targeted functionality, a tactical keypad, and enhanced connectivity. Because the devices are touch-based, they are more familiar to the user, which improves speed to productivity.

ASSET MANAGEMENT AND ANALYTICS

Do you know where your devices are in the hospital or how your clinical staff is treating them? Consumer devices can be complicated to track and are not set up for real-time analytics. Honeywell provides Operational Intelligence software for your healthcare enterprise devices. Your IT staff will have access to actionable insights that can help answer critical questions. The cloud-based solution enables deeper insights into your clinical workforce – from basic device usage tracking to detecting potential abuse of company assets and more – so your healthcare organization can maximize the value and longevity of your device lifecycle and keep your staff focused on patients. Newer features of Operational Intelligence for healthcare providers give greater visibility over social distancing and implement additional cleaning protocols.

LIFECYCLE MANAGEMENT IS A KEY DIFFERENTIATOR

3

Product lifecycle is the key differentiator between consumer devices and healthcare enterprise mobile computers. Healthcare decision-makers need to factor in the true-life expectancy of devices used by their hospital clinicians/staff. There several variables for consideration that have a direct bearing on TCO.

According to VDC, consumer devices have a failure rate of 2 to 2.9 times greater than purpose-built medical grade device.

Consumer devices have a much shorter timespan before they are supplanted by a brand-new model, whereas healthcare enterprise devices are designed to provide many years of service. According to VDC[1], these devices have a failure rate of 2 to 2.9 times greater than purpose-built medical-grade devices. Causes of failure include constant hazard exposures and disinfection requirements, hardware-specific (e.g., drops) failures, software and application failures, failures to network connectivity. The higher the failure rate, the larger the spare pool is required to mitigate lost productivity.

Instead of deploying a healthcare enterprise device, some organizations choose consumer devices and budget accordingly for the shorter lifecycle. While this strategy eliminates the surprise of replacement costs, you would need to forecast device cost over a certain period to ensure a cost-competitive option vs. a healthcare enterprise device.

Even healthcare organizations that plan for a consumer device refresh – something they'd typically have to do twice as often as an enterprise device – often overlook the associated cost and disruption in device availability. The new devices must be purchased, shipped, stored, tested, configured, and more. Also, old devices must be returned. Experienced organizations may handle these efforts well, but they still bear the cost. It's also worth noting that once a device reaches the end of life (EOL), so will the spares and accessories available for it.

Medical enterprise devices are designed to provide many years of service and have replacements, spares and repairs factored into the design process. This ensures that the device offers maximum service time before replacement.

Honeywell Mobile Computers are based on the **Mobility Edge Platform**, a locked-down, integrated, HW-SW core that enables us to deliver rapid innovation across multiple form factors, best-in-class security, unbeaten product life and uninterrupted operating system support. Users of Mobility Edge devices enjoy unbroken Android version continuity.

1. VDC Research Group, Inc. | Enterprise Mobility, "Total Cost of Ownership Models for Line of Business Mobile Solutions," December 2018.

MOBILE DEVICE REPAIRS AND SPARES

Every time devices need to be replaced due to breakage or failure, healthcare organizations incur costs and delays related to device configuration and deployment, in addition to the direct cost of purchasing the new device.

The higher the failure rate for a category of devices, the larger the spare pool the organization should keep on hand to mitigate lost productivity when devices fail. Adding to the spare pool adds to the overall acquisition cost, but not the per-unit acquisition cost, and thus may be overlooked in some cost comparisons.

It is important to note that healthcare enterprise devices are designed to be repairable. Manufacturers, like Honeywell, typically have mature service programs and infrastructures that can contractually commit them to quickly provide replacement devices and complete repairs in a timeframe that is acceptable to the organization buying the devices.

BACKWARD COMPATIBILITY

Once consumer-grade devices have reached the end of life, there is no guarantee that the next model will provide backward compatibility for accessories and applications. This means you can get a mix of devices, andaccessories in your inventory.

Because Honeywell is focused on healthcare needs instead of consumer needs, when the next generation of devices is released, you can usually count on the backward compatibility with applications to accessories such as batteries, cables, cradles. That means you can upgrade to the next generation of mobile technology and preserve your existing investments as possible. Healthcare enterprise devices are usually are available for an additional period of years once they are discontinued.

SUPPORT SERVICES ESSENTIAL FOR LIFECYCLE MANAGEMENT

What happens when a mobile device fails? Can you get the same level of service for a consumer-grade device that you can for a medical-grade device? Once a healthcare enterprise procures an asset or service, they experience many stages of mobile fleet management that are managed across various departments. Many hospitals would have great difficulty offering a 24x7x365 support team with the needed breadth and knowledge depth.

At Honeywell, we support national, multinational or global enterprises with our world-class Managed Mobile Services (MMS) with over 1.9+ million devices that are under-managed agreement. We have a birds-eye view regarding the pros and cons of how to manage a mobile estate of varying complexities best. We have helped some customers reduce their network and mobile expenses by 20-30%.

Honeywell MMS supports healthcare-liable devices and individual-liable BYOD (Bring Your Own Devices) that employees use to access company resources and information. When you outsource support to a quality provider, like Honeywell, you can expect a mobile service center to handle all your service needs because they support multiple enterprises and have the volume to provide a lower management cost per device.

THE FACTS: ENTERPRISE MOBILITY SOLUTIONS OFFER BETTER TCO

4

At Honeywell, we have been working closely with our healthcare customers to help them realize the optimal performance of enterprise devices across all healthcare environments. Throughout this whitepaper, we have sought to share just a few of the critical issues healthcare decision-makers need to evaluate when considering consumer devices vs. enterprise devices. We strive to offer a mobile solution that will exceed expectations, provide optimal satisfaction among users in every healthcare use case, and actual cost savings when looking at the investment from a capital expenditure (CAPEX) and the day-to-day operating expenses (OPEX) incurred through using enterprise devices.

A total cost of ownership (TCO) analysis provides essential insight for aligning the 'right' mobile solutions with the target application or use case. You can genuinely assign value to the mobile device as a solution over the narrow focus at the upfront cost. This reduces the risk of a failed or poorly performing mobile solution that disrupts workflow productivity and increases the overall TCO.[1]

Gartner says, "Ruggedized (enterprise) equipment tends to be significantly more expensive than commercial off-the-shelf (COTS) devices – typically 2.5 to three times more expensive when comparing list prices. When doing a full total cost of ownership (TCO) calculation, ruggedized equipment often comes out as having a lower or equal TCO, due to its longer life and the use of a single device across multiple (shift) workers. Customers often focus solely on the ability of the device to withstand drops, and, as such, believe that regular devices enclosed in a case, at a lower cost, could suffice. This may be true in some situations, but many other factors need to be considered regarding truly ruggedized devices."[2]

The difference between hard costs and soft costs shows why product comparisons and TCO evaluations should not be based primarily on mobile computer list prices and other hard costs. Soft costs have a much more significant impact on the total cost of ownership than hardware acquisition costs. At Honeywell, we have a front-seat view of the TCO healthcare organizations are experiencing because of the soft costs. Consider the following from VDC.[3]

1. VDC Research Group, Inc. | Enterprise Mobility, "Total Cost of Ownership Models for Line of Business Mobile Solutions," December 2018
2. Source: Gartner, Revisit Your Ruggedized Strategy Before You're Hit by the End of OS Support, Leif-Olof Wallin, Stephen Kleynhans, et al., Published March 27 2017
3. VDC Research Group, Inc. | Enterprise Mobility, "Total Cost of Ownership Models for Line of Business Mobile Solutions," December 2018

CONSUMER DEVICES REFRESH AT 18 MONTHS

Consumer-grade devices need refreshing beginning at 18 months, while purpose-built devices start needing to be refreshed at 5-plus years.[1]

CONSUMER DEVICES FAIL 2.9 TIMES MORE OFTEN

Mobile computers cost the most, not when they're purchased or replaced, but when they fail. Failure rates of consumer-grade devices are 2.9 times higher than enterprise devices. Causes of failure are far-reaching and include: [1]

- Hardware-specific failures (dropping the device, water, temperature, vibration). For example, while consumer devices are paying more attention to design features related to IP67, they fall short in areas of drop protection because of the increased use of glass.
- Software and application failures to network connectivity.
- Battery performance because 75% of batteries do not last an entire shift, and batteries erode over time and are not be replaceable. Consumer batteries need to be replaced every 14 months compared to 3 to 5 years cycles for enterprise mobile computers. Organizations overcompensate by having a larger than required spare pool of devices and batteries.
- Environmental conditions such as poor interfacing with a device when using gloved or wet hands, in direct sunlight or extreme temperature and vibration.

Also, the increased failure rate raises the cost of buffer/spare pool stock needed to replace a broken device when one is being fixed. The greater the device failure rate, the bigger and more expensive buffer is required.

LOSS OF WORKER PRODUCTIVITY

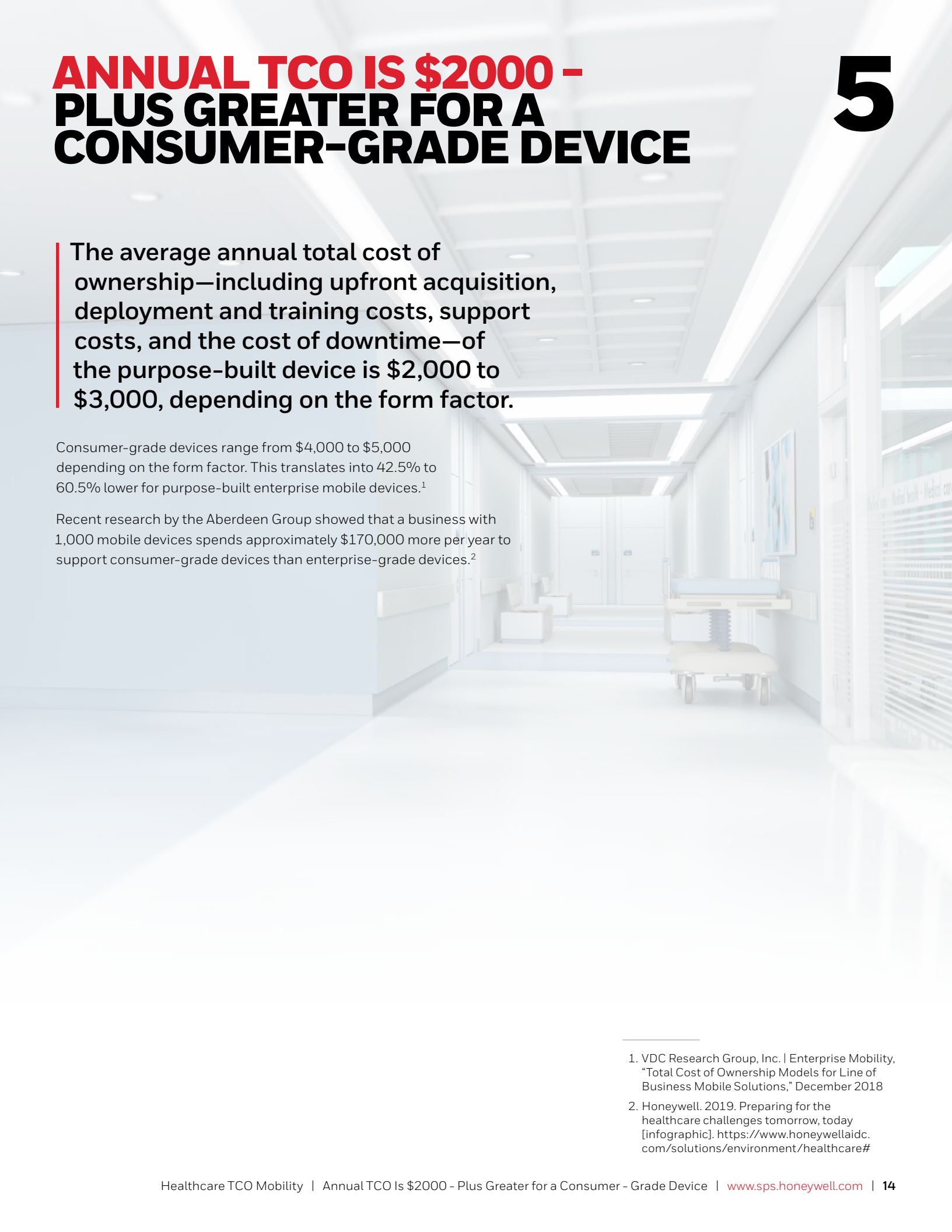
The most significant contributor to mobile device TCO is the mobile worker's loss of productivity and the time and staff required to support mobile devices. Each device failure results in 60 to 110 minutes in lost worker productivity. Another 40-60 minutes are typically lost in IT support for each mobile solution failure. Soft costs occur because of: [1]

- Carrier and administrative costs associated Helpdesk and associated tools. Consumer devices generate more calls resulting in overall high charges.
- Device commissioning time and cost. Some consumer devices can only be commissioned one at a time. Fixing a mobile solution including a software reload averages 87 minutes.
- Costs of staff and non-staff in the refresh cycle of buying, storing, building, planning, deploying, recovery old kit and disposal.
- IT staff's inability to remotely update/redeploy software, view or interact with a device, properly diagnose problems, review device logs.
- The worker continues working with pen and paper until they can access a new device.

1. VDC Research Group, Inc. | Enterprise Mobility, "Total Cost of Ownership Models for Line of Business Mobile Solutions," December 2018

ANNUAL TCO IS $2000 – PLUS GREATER FOR A CONSUMER-GRADE DEVICE

5



The average annual total cost of ownership—including upfront acquisition, deployment and training costs, support costs, and the cost of downtime—of the purpose-built device is $2,000 to $3,000, depending on the form factor.

Consumer-grade devices range from $4,000 to $5,000 depending on the form factor. This translates into 42.5% to 60.5% lower for purpose-built enterprise mobile devices.[1]

Recent research by the Aberdeen Group showed that a business with 1,000 mobile devices spends approximately $170,000 more per year to support consumer-grade devices than enterprise-grade devices.[2]

1. VDC Research Group, Inc. | Enterprise Mobility, "Total Cost of Ownership Models for Line of Business Mobile Solutions," December 2018
2. Honeywell. 2019. Preparing for the healthcare challenges tomorrow, today [infographic]. https://www.honeywellaidc.com/solutions/environment/healthcare#

CONCLUSION

At Honeywell, we focus on helping you provide high-quality patient care and supporting you in your patient-centered approach. This includes the latest technology that is purpose-built for the clinical environment.

Together, with our strong partnerships with healthcare leaders, we're facilitating an ongoing technology evolution and redefining what's possible for healthcare organizations of all shapes and sizes. We believe the most innovative technology knows how to stay out of your way, so you can focus on what's most important – delivering the best-in-class care your patients expect.

To learn how to help transform your patient care through the latest technology solutions, contact a Honeywell representative at 800-537-6945.

For more information

www.sps.honeywell.com

Honeywell Safety and Productivity Solutions
300 S Tryon St Suite 500
Charlotte, NC 28202
800-582-4263
www.honeywell.com

Healthcare TCO Mobility WPR LTR | RevA | 06/21

Honeywell