Considerations for Endpoint Management Strategies for Healthcare Workers

Prepare your infrastructure for the growing IT-service demands of healthcare worker’s mobility

Introduction

Having a company cell phone and being able to communicate with colleagues independently of a stationary work space is essential for modern healthcare workers.

In this paper we take into consideration the data security, privacy, legal, IT-infrastructure, device lifecycle and service management needs that could arise from the growing popularity of work cell phones.

The purpose of this document is to inform IT experts and IT stakeholders about aspects, possible solutions and possible effects related to mobile device usage in healthcare environments.

Use Cases for Mobile Devices in Healthcare

A doctor needing access to a medical app that provides a quick overview of the side effects of a certain drug, a nurse coordinating their shift schedules with their team members or a call to a different clinic department for arranging the transfer of a patient. There are a lot of possible use cases of mobile devices in the healthcare system that make navigating common processes more efficient.

Challenges in Equipping Workers with Mobile Devices

Not every healthcare worker can be equipped with an organization-owned mobile device though. If the financial burden on clinics of having to invest in new devices is not enough of a factor to steer the decision, the additional strain on the clinic's IT-department having to manage each device's lifecycle and the growing potential for IT-security related incidents, will certainly be.

Data Security Concerns

A lot of healthcare workers might resort to using their personal devices for meeting those daily challenges in communication, coordination, and decision-making.

If the overwhelming majority of workers are using these digital tools to help them in their workload, it would be difficult to argue with specific users to stop and consider the data security related issues stemming from using their personal devices.

Mobile Device Management (MDM) tools typically used by companies, are tools that support IT-teams in the lifecycle management, the installation, the deployment, the onboarding, the remote configurations and the reporting of their organization's mobile devices.

Mobile Device Management as a Solution

Having to invest in integrating a new MDM solution also has its own challenges. The license cost on one hand, but also the additional trainings for each service aspect of the IT-Department. Helpdesk agents might need to be able to perform certain actions in the MDM tool, other's have to take care of the helpdesk agents access to the MDM tool, while the IT-Manager would need access to reports and others might be responsible for the MDM tool's functionality (i.e. if it's an on-premise solution, installation of service updates, server up-time, contacting vendor support etc.).

Lessons from other Industries

There has to be a specific demand for such a solution, balancing the efforts of maintaining it.

As you can imagine the corporate world, with workers in different roles of a company, from sales departments and customer communication, to frontline workers and specific applications designed for their daily work, has a well-founded interest in MDM tools and being able to equip their employees with their own mobile device in a quick, simple and streamlined manner.

There are a lot of lessons that have been learned, best practices and standards, clear and concise recommendations, well thought out considerations and a profound experience in every aspect and effect of organizationally provided mobile devices that the healthcare system could benefit from.

From nurses personal mobile devices being registered as such, virtually divided in personal and work related containers without the organization having access to the personal container or the overall device's features in general to completely organizationally owned and remotely managed strictly for work usage configured devices, that can be wiped or located in a matter of seconds if it was lost.

The Debate on Restrictions

There is a broad spectrum of different restrictions in mobile device usage and regulatory considerations that differ from each business sector. But there are also a lot of basic commonalities. One of them is the general question overarching most debates about setting a restricting configuration on a device: we could change this setting from a technical side, thereby restricting certain actions for users on the device, or we could tell users to avoid performing certain actions. This argument seems to come up mostly in the realm of smartphones. The question if we could simply tell users to comply to our verbal or even written agreement, has no effect on malicious intruders gaining access to these computers. Therefore in the realm of managing desktop computers or notebooks, the question “how can we set this restriction from a technical side?” is certainly more commonly asked than “can we instead simply tell the user to avoid this certain action?”.

Expanding IT Awareness

The understanding, the experience, the knowledge and the lessons, the longstanding effects and even the worst outcome of an unmitigated vulnerability, IT-Departments have in regards to desktop computers and notebooks, has to breach the world of mobile phones and other mobile devices. Even smart watches, entertainment systems, car radio compatibility.

The knowledge transfer between companies, organizations, sectors even, has its pitfalls with regards to privacy and transparency into each organization’s processes. But the advantages in modernizing workplaces as we know them, with the help of experts, consultants and engineers, is one way to avoid these pitfalls and reduce risks of these liabilities.

Conclusion

To successfully integrate mobile device management in a healthcare setting, organizations should:

- Define clear Bring-Your-Own-Device (BYOD) policies that balance flexibility and security
- Implement MDM tools tailored to the specific healthcare environment
- Provide comprehensive IT training for proper security enforcement
- Leverage insights from other industries to refine best practices

By adopting these strategies, healthcare organizations can ensure a secure, efficient, and modern mobile infrastructure without compromising data protection or regulatory compliance.

Legal Disclaimer

This document is provided for informational purposes only and does not constitute legal advice. While efforts have been made to ensure accuracy, we do not guarantee completeness or applicability to specific circumstances. Service providers operating in Germany must comply with the Telemedia Act (Telemediengesetz - TMG) and relevant data protection laws, including the General Data Protection Regulation (GDPR).

Any information regarding IT infrastructure, mobile device management, and data security should be verified with legal professionals or relevant authorities. We assume no liability for direct or indirect consequences resulting from the use of this document.

For further details on compliance requirements, please refer to official sources such as the German Federal Network Agency (Bundesnetzagentur) or consult a qualified attorney.