ORIGINAL ARTICLE

Challenges and opportunities in achieving secure hospital clinical mobility management: An illustrative use case

George A. Gellert*[1], Glynn Stanton[2], Michael Paulemon[2], Mark Roberts[2], Robert Hardcastle[2], Sean P. Kelly[1,3]

[1] *Imprivata, United States*
[2] *Yale New Haven Health System, New Haven, CT, United States*
[3] *Beth Israel Lahey Health, Harvard Medical School, Boston, MA, United States*

Received: February 16, 2024 **Accepted:** April 17, 2024 **Online Published:** April 24, 2024
DOI: 10.5430/jha.v13n2p1 **URL:** https://doi.org/10.5430/jha.v13n2p1

ABSTRACT

Objective: To qualitatively describe a use case at Yale New Haven Health System (YNHHS) illustrating the need for and effective deployment of innovative technologies to manage an enterprise-owned shared device (EOSD) management program. EOSD management provides clinicians with secure, rapid access to enterprise mobile devices and applications, maintains devices in functional, use ready condition for clinicians, and enables enterprise tracking and reduced loss of devices.

Methods: Executive leaders in clinical information technology and informatics management at YNHHS were interviewed through written and telephonic communication. Qualitative data was gathered through communications between clinical and information technology executives and the implementation support team of a leading identity and access management (IAM) solutions and EOSD management solution provider. Use case information was gathered, integrated and shared with health system executives and health IT/informatics leaders to verify the description of unmet needs, solution objectives and impact/value delivered after implementation of the EOSD management solution.

Results: Benefits realized from implementation of an enterprise-shared mobility management solution included establishment of a cohesive and comprehensive enterprise-owned, shared device management strategy. This included effective monitoring and dynamic management of the system's mobile device fleet, and better IT resource management with reduced mobile device loss. The IT administrative burden was reduced. While not surveyed systematically, improved clinician experience and satisfaction were reported to IT leaders anecdotally. EOSD management solution deployment was rapid, as was the time to improved clinician mobile experience and clear demonstration of value.

Conclusions: A leading US health system was able to rapidly deploy a shared mobile device management solution that enabled effective monitoring and dynamic management of the enterprise mobile device fleet, with easier and faster clinician device access and workflows, and reduced IT administrative demand and costs. While the complexities associated with increased clinical mobility in healthcare will likely continue to grow, issuing future device and mobile management challenges that require effective hospital system response, technologies have emerged that enable more effective, efficient and satisfactory organizational mobility performance.

Key Words: Mobile device access, Clinical mobility, Mobility, Mobile device management, Identity and access management

*__Correspondence:__ George A. Gellert; Email: ggellert33@gmail.com; Address: 703 Sentry Hill, San Antonio, TX 78260, United States.

1. INTRODUCTION

Healthcare delivery organizations (HDOs) are seeking new methods to simplify and streamline point-of-care workflows, and many are implementing mobility projects to address enterprise-wide initiatives. Mobile devices facilitate and optimize the expanding Internet of Medical Things (IoMT) by streamlining many workflows at the point of care and enabling fast, secure and real-time transfer of patient data across the connected network. Recent innovations in interoperability have made it possible to enable more clinical workflows at the bedside using mobile technology. Growth in use of mobile devices by nurses and physicians is expected to continue.[1]

HDOs require mobile tools that improve workflow flexibility, particularly as budgets and human resources are increasingly constrained. Achieving efficient workflows on mobile devices with minimal diminishment of security or privacy is a substantial challenge. Enhanced security measures can hinder usability and adoption, such that HDOs struggle to optimize investments in mobile technology. Digital identity needs to be leveraged to ensure security and eliminate barriers that impede usability. HDOs must simultaneously reduce points of exposure and ensure the highest quality of care delivery with secure access to essential tools and patient data 24/7/365 and anywhere. This discussion will examine the reasons for the rapid rise in the use of mobile devices and why they are viewed increasingly as critical assets for clinically- and cost-effective operations, and will consider how hospitals can better leverage their investments in mobile technology as they concomitantly ensure security and ease adoption of enterprise-owned devices.

2. BACKGROUND: WHY CLINICAL MOBILE DEVICE USE IS INCREASING AND WARRANTS IMPLEMENTING A SECURE AND EFFECTIVE MOBILITY STRATEGY

Diverse HDO needs and considerations are driving and shaping the increased use of mobile tools among clinicians, as summarized in Table 1.

2.1 Need to improve smart device interoperability as the IoMT expands

The IoMT has rapidly increased the number of connected devices and applications in healthcare, while also increasing care efficiency. It's expected that the number of IoMT devices globally will grow 131% by 2026.[2] Mobile devices can help facilitate and optimize the expanding IoMT by streamlining many workflows at the point of care, which enables faster secure real-time transfer of patient data and access to the connected network.

2.2 Need to improve anywhere access to secure enterprise-managed and personal devices

When HDOs enable clinicians to engage workflows extending beyond the primary organizational footprint, it is essential that information security/privacy are in place protecting everywhere staff accesses confidential data/information. To securely deliver the needed features of mobile technology, HDOs must ensure rigorous authentication in a manner promoting ease of use. Digital identity is central to supporting these processes, and enables the enforcement of mobile device security by establishing effective passwords and authentication that is not disruptive to efficient clinician workflows. Accessing confidential information using mobile-based authentication modalities is a key requirement.

Table 1. Key health system drivers and needs as mobile technology use increases

Key Health System Mobile Technology Drivers and Needs
Why mobile device use is increasing:
• Improve access to and security on enterprise-managed and personal devices
• Leverage mobile technology to increase care efficiency
• Create a seamless clinical-user experience
• Reduce clinician and IT fatigue and professional burnout
• Reduce device fleet and IT system costs
• Increasing budget expenditures to replace hardware for workstations on wheels, computers in patient rooms, and barcode scanners which can be replaced by mobile devices
Benefits of implementing enterprise mobile device management:
• Streamline access and device management
• Improve access and security on personal devices as clinical and IT burden increase
• Better balance security and privacy compliance with workflow flexibility
• Enable privacy in shared-use environments
• Improve interoperability as the IoMT expands

2.3 Need to leverage mobile technology to increase care efficiency

Providing new mobile technologies to clinicians enables faster care delivery to patients. An evaluation of how mobile devices affect patient satisfaction found that 96% of organizations that implemented mobile devices observed improved patient satisfaction/experience scores.[3] Further, 72% of organizations indicated that improved quality of patient care

ISSN 1927-6990 E-ISSN 1927-7008

was a direct result of enabling clinician mobility. As HDOs work to streamline clinical workflows by deploying greater mobility, clinicians can spend more time face-to-face with patients and their families, contributing to improved patient experience and satisfaction, and allowing for better quality of care delivery for a higher number of patients each day.

2.4 Need for streamlined access to and management of mobile devices

By leveraging available authentication methods on clinicians' mobile devices, including proximity card, soft tokens, biometric identification and facial recognition, HDOs can support secure, efficient, and easy mobile access. Supporting trusted authentication on mobile devices and applications is now possible thanks to digital identity platforms, which also enable HDOs to establish audit trails documenting which clinician used a particular device at a particular time, at what location and for what duration, thus helping to diminish the loss rate of devices. Reducing barriers to secure access can be achieved through the effective deployment of digital identity and mandatory authentication at the device and application level, enabling HDOs to ensure security in bring your own device (BYOD) and shared-use settings that is frictionless.

2.5 Need for a clinical user experience that is seamless

Employing existing authentication workflows that are well familiar to clinicians on their mobile devices enhances user experience. For shared environments the challenge centers on achieving a personalized experience without repetitive manual workflows, regardless of what device is in use. For personal devices, HDOs need to enable mobile device access through a trusted, seamless second factor authentication. Secure access to critical tools must be supported for all relevant locations around the clock, while achieving full compliance with Drug Enforcement Agency (DEA) or other regulatory authority regulations for such applications as electronic prescription of controlled substances (EPCS).

2.6 Need to reduce clinician IT fatigue and professional burnout

Inadequate staffing levels and insufficient time spent with patients often contributes to fatigue and professional burnout. According to a report done by the American Nursing Association, 89% of respondents shared that their organization is experiencing a staffing shortage.[4] One method to help reduce clinician burnout is to simplify and streamline IT and clinical workflows at the point of care by ensuring increased availability of clinical information and expanded device functionality. Furthermore, clinicians benefit from an expanded ability to share information more quickly, improving communication and coordination across multidisciplinary care team members. Easing and expediting real-time mobile access to confidential patient information while providing care improves clinician efficiency and productivity. Simplifying and expediting clinician management of alarms, administration of medications, and other time-sensitive tasks through mobile device use improves point of care delivery, and enhances clinician experience and satisfaction.

2.7 Need to reduce capital and operational costs for IT teams

Mobile devices are less expensive to purchase, manage, and maintain than traditional desktop environments.[5] Standardizing technologies that can be shared between clinicians is cost-effective and requires less effort from IT teams as efficiencies of scale are created managing fewer devices and unique environments. In addition, with distributed mobile device docking stations across hospital units, greater ease of mobile access to the EHR helps maximize its appropriate utilization, and expands value derived from a significant EHR investment.

2.8 Need to improve information access while maintaining security posture and reducing IT administrative burden

As the number of smart devices grows, ensuring that connected devices in the healthcare environment are properly secured against potential threats is a daunting task. This complexity is compounded when devices support access to many workflows and more sensitive information, and are shared across different clinical resources. A reported 67% of HDOs recognize that data privacy is a top concern for mobile devices.[3] Given US Department of Health and Human Services (DHHS) recent advisories around HIPAA compliance for connected devices in healthcare settings,[6] keeping accurate audit trails of inventory and security measures for mobile devices is more important than ever. HDOs must meet the challenge of tracking which users had access to which devices at a particular time and for what purpose. There is increasing need for comprehensive, end-to-end mobile management solutions that facilitate HDO optimization of their mobile deployment, including delivering automated device provisioning, secure device checkout and secure, rapid user access. Thus, HDOs face a formidable challenge in unlocking the full potential of shared mobile devices because of the imperative to ensure expedited, efficient workflows while simultaneously improving security and auditability.

2.9 Need to better balance security and privacy compliance with workflow flexibility

Security assurance processes can hinder usability and adoption, causing sub-optimal return on HDO investments in

mobile tools. Ensuring mobile device security/privacy with minimal impact on clinical workflow efficiency can be challenging in enterprise-owned device and BYOD settings. Supporting security and compliance directly within mobile workflows by leveraging digital identity enables HDOs to reduce friction that negatively impacts usability and diminishes exposure and adoption risk by ensuring secure access to needed information and tools in real-time.

2.10 Need to enable privacy in shared-use environments

When resources are shared among users, HDOs need to support personalization and privacy in a shared enterprise-owned device environment. Leveraging digital identity to enable trusted access to devices/applications is possible using modalities such as badge-tap device assignment, which lock down shared devices and prevent unauthorized access between users.

3. RESULTS

3.1 Study objectives

To qualitatively describe a use case at Yale New Haven Health System (YNHHS) illustrating the need for and effective deployment of innovative technologies to manage an enterprise-owned shared devices program. Enterprise-owned shared device management provides clinicians with secure, rapid access to enterprise mobile devices and applications, maintains devices in functional, use ready condition for clinicians, and enables enterprise tracking and reduced loss of devices.

3.2 Setting

Yale New Haven Health (YNHHS) is a large comprehensive healthcare system in Connecticut delivering clinical care services through five hospital facilities and employing over 37,000 individuals, including more than 7,500 university-affiliated and community-based physicians and advanced care practitioners. The study interviews were completed during September 2023 and collated and validated that October. Primary interviews were collected from the management of the health system's Digital and Technology Solutions team, collated and documented, with review and validation of content by other key members of the technical teams responsible for implementing and supporting the new shared mobile solution. From a device standpoint, YNHHS encompasses over 35,000 workstations and over 10,000 mobile devices (all iOS operating system Apple devices, including iPads as well as iPhones).

3.3 Study design

Executive leaders in clinical information technology and informatics management at YNHHS were interviewed through written and telephonic communication. Qualitative use case data was gathered from interviews and correspondence with YNHHS clinical information technology executives, managers and staff and representatives of a leading identity and access management (IAM) solutions and EOSD management solution provider. The interview, conducted by teleconference, was comprised of 15 initial questions that were shared in advance, including follow up queries and confirmation of information conveyed, and was recorded. Interview duration was 60 minutes. Interview content was transcribed for validation and documentation purposes.

Use case information was gathered, integrated and shared with the participating health system executives and health IT/informatics leaders to validate the descriptive accuracy of unmet needs, solution objectives and impact/value delivered following implementation of the EOSD solution. Recommended changes in use case content were completed, and a final report was shared with executive and health system IT/informatics stakeholders for final review and approval approximately four weeks after the interviews were conducted. Minor edits based on feedback from the health system were received two weeks later, along with authorization to publish the findings.

3.4 Yale New Haven Health System clinical mobility and IAM needs

Prior to implementing an advanced enterprise-owned shared device solution, YNHHS had a need to systematically and effectively manage a large fleet of shared smartphones across five hospitals. In achieving the latter, a high priority was to simplify IT operations, while both ensuring a positive clinician experience/satisfaction and safeguarding patients' personal health information (PHI). In 2022, YNHHS initially introduced in excess of 6,000 enterprise iPhones during implementation of a new mobile collaborative clinical communications application at the system's five Connecticut hospitals. Previously, YNHHS IT services utilized a mobile device management (MDM) platform to enroll, configure and track hospital iOS mobile phones, which was time consuming and manually intensive.

The average HDO in the US experiences an annual mobile device loss rate of 15%-20%.[7] With a similar device loss rate, YNHHS IT leaders recognized that in the absence of effective monitoring capabilities, the system would be inefficient in tracking and replacing lost iPhones. It needed to ensure that the health system would never face a scenario where there were insufficient devices on hand to satisfy clinician demand for mobile smartphones. In addition, YNHHS IT services sought the ability to lock a mobile phone if not checked back in within a specified time (48 hours beyond

the scheduled return time).

3.5 Description of secure mobile access and control technologies deployed

A cross-departmental technology evaluation committee, composed of representatives of client services, information technology, mobile solutions, clinical informatics and clinicians, examined available mobile management solutions. The committee compared key technology and functional features, implementation capabilities, and ongoing technical support from solution providers. In particular, a mobile solution needed to have substantial growth capacity and a clear roadmap of how the solution would evolve in the future. YNHHS implemented Imprivata solutions to support a secure, consistent workflow experience across all mobile devices used to access their applications and clinical information. For shared device workflows, Imprivata GroundControl was the EOSD management solution used to automate smartphone provisioning, and to provide a comprehensive access control solution that would streamline mobile device access and authentication. This offered cloud-based management tools to enable easy tracking, support and maintenance of dispersed mobile assets.

GroundControl was integrated with the existing, earlier implemented Imprivata OneSign single sign-on solution, which enabled a rapid, familiar, and consistent authentication process for clinicians on clinical workstations, virtual desktops, and mobile phones. Thus, clinical users would engage the new EOSD management solution using secure access technology and a workflow that they were already well familiar with and actively using. Mobile device access was identical to the process that clinicians used to access the organization's clinical workstations, the health system EHR, and other clinical applications.

IT administrators could establish user authentication polices across systems and varied workflows from a centralized platform to improve reporting compliance and reduce ownership total cost. IT resources required to administer and manage authentication workflows decreased. Users could access shared mobile devices with a proximity identity badge tap, and quickly access their applications, removing the need for manual authentication, much as they did to the organization's EHR and other clinical applications.

The Imprivata GroundControl EOSD management solution supported cloud-based device management and could be maintained and updated from any location 24/7/365. YNHHS benefited from personalized device checkout, and ease of application access. For physicians accessing PHI from a BYOD personal device, Imprivata Confirm ID for Remote Access improved security by enabling enterprise-wide two-factor authentication for remote network access, cloud applications and Windows servers and desktops. Imprivata Confirm ID for EPCS provided the broadest range of DEA-compliant two-factor authentication modalities, including hands free authentication (HFA), push token notification, and fingerprint biometrics in order to ensure that EPCS is fast and convenient for providers.

Because YNHHS is a multi-hospital system comprised of various facilities spread across a large geographic service area, implementation planning with the solution provider involved early formal and planned enterprise-wide communications about the EOSD management solution in a timely and consistent manner. IT administrative leaders and staff emphasized that this would reduce potential concerns or resistance to the deployment. In addition, standard user training content on the new mobility solution was conveyed by the solution provider to YNHHS, which its training team integrated and disseminated by both a PowerPoint presentation and a video posted on the system's internal intranet. This included a profile summary of the applications that would be available on mobile devices as managed by the Imprivata Ground Control solution.

4. RESULTS

YNHHS IT/informatics leaders reported a diverse range of interrelated benefits from implementing the advanced enterprise-owned shared device management solution, as shown in Table 2 and described below.

Table 2. Benefits realized from implementation of an enterprise-owned shared mobility management solution

Key Health System and Hospital Benefits Realized
• Enabled a cohesive/comprehensive enterprise-owned, shared device management strategy
• Anecdotal reports of improved clinician user experience and satisfaction
• Effective monitoring and dynamic management of system's mobile device fleet
• Better IT resource management and reduced mobile device loss and associated costs
• Reduced IT administrative burden and clear return on investment
• Rapid time to value demonstration and improved clinician mobility workflow
• Rapid deployment and effective collaboration with solution provider
• Future expanded utility and value growth potential

4.1 Enabling a cohesive and comprehensive enterprise-owned shared device strategy

In planning such a major rollout, YNHHS IT/informatics executives reported that the organization recognized, prior to the implementation, that a systematic strategy for shared device management was needed. Having the ability to systematically, rapidly and efficiently provision, maintain, and audit a large number of mobile devices was essential. After evaluating available potential solutions on the market, the GroundControl shared device management solution from Imprivata was selected and implemented across the system to enable effective management of the expanding mobile device fleet. YNHHS leaders reported that this was accomplished successfully, and the EOSD management solution was integrated with the existing MDM solution deployed within the YNHSS IT system. The solution was reported to have improved visibility, security and optimal management of the device fleet.

4.2 Effective monitoring and dynamic management of system mobile device fleet

After implementation, YNHHS IT/informatics leaders reported that the shared mobile management solution made it easier to track check-ins and check-outs of 6,000 enterprise mobile devices, and improved device accountability and reporting mechanics. EOSD management yielded estimated annual recurrent cost avoidance and savings of $500,000 due to reduced device loss, with fewer lost or stolen devices following implementation. This estimate was based on a per device cost of $284, encompassing fractional IT staff time reduced for device loss detection and reporting, replacement and redeployment. These value estimates do not factor in consideration of the lost productivity of the clinical department affected by a device loss, but presumably if it were possible to estimate and quantify this systematically, it would increase the impact and value conveyed by the EOSD management solution. The baseline device loss rate fell from 1,260 to 240 devices, or from 21% to 4% in absolute terms (a relative decrease of 81%). Importantly, these device numbers are not static, and devices were added over the course of and subsequent to EOSD solution implementation. Device loss rate increased during the biannual device refresh. Thus, the estimates conveyed should be regarded as conservative and minimal cost avoidance and savings achieved.

Increased IT/informatics agility was evident in more rapid mobile device setup and deployment. Improved IT team productivity resulted, as informatics team members were able to focus on more strategic tasks and needs. The burden on the IT help desk decreased soon after initial implementation, with fewer mishaps, incoming questions, and problem tickets opened by clinical users. Anecdotally, clinicians reported a superior user experience to their departmental leadership, noting that badge-tap device access was effortless, convenient, and rapid.

4.3 Better IT resource management and reduced mobile device loss and associated costs

YNHHS clinical informatics leaders reported that with the increased automation provided by the EOSD management solution's functionality, IT productivity and clinician efficiency improved, enabling the organization to maximize the value derived from its investment in mobile technology and its unified communications solution. By automating routine provisioning functions, system IT administrators easily deployed smartphones across all five YNHHS hospitals. System IT/informatics administrators reported more granular visibility and effective control across the mobile device fleet. This greatly simplified management of mobile assets, and an estimated 15%-17% relative reduction in smartphone loss and theft was observed from the prior device loss baseline level of 20% per year (or 75%-85% reduction in absolute terms). In addition, IT administration reported that the EOSD management solution enabled easier real time monitoring of the staff to mobile device ratio across the system.

Loss detection also became a real time rather than periodic assessment. With the new solution, the IT department was able to rapidly contact the last individual that checked out an overdue device, or escalate if needed an inquiry to the departmental manager regarding the status of the device and its expected return. In addition to cost savings from a reduction in mobile device loss rate, cost avoidance and savings to the system were realized by not retaining a particular telephone line in connected/functional status and generating monthly service fees for what in the past was as long as 2-4 months until the device was substantiated and classified as lost. YNHHS estimated that the annual cost savings of replacing lost devices plus reducing the length of time until a line is disconnected was roughly $400,000-$500,000 per annum. In addition, IT staff time receiving, evaluating, and acting upon missing device service tickets decreased substantially. Time spent determining where a reported lost device may be located and seeking approval for and re-ordering a new replacement device from the system's smartphone carrier also meaningfully decreased, with IT staff able to focus on performing other needed activities and tasks instead.

Clinicians gained instant access to devices, which eliminated workflow friction and increased user satisfaction, with clinicians reporting anecdotally to clinical leaders a superior device use experience, and this drove technology adoption. In addition, IT team members perceived that clinical users of mobile devices had acquired a greater sense of accountability

for devices loaned to them following the implementation of the EOSD management solution, and that as a result, had become more conscious of the need to monitor and securely maintain their loaned device.

4.4 Reduced IT administrative burden and clear return on investment

IT/informatics leaders reported that the solution minimized manual administrative processes, helped simplify IT operations, avoided/reduced problems in provisioning, and reduced the demand for and frequency of IT help desk interactions. The informatics team spent more time focused on strategic concerns supporting the system in key areas and less configuring or tracking potentially lost devices. For example, following implementation iOS updates and other administrative workflows were automated while mobile phones recharged. Asset management tools and status notifications that are cloud-based inform the system IT/informatics team proactively to enable effective monitoring of iPhone health and status data, to track devices, and to minimize inventory loss. The time required for IT team members to contact and engage clinical staff to validate the status of a particular device was reduced substantially.

4.5 Rapid time to value demonstration and improved clinician user experience

YNHHS IT/informatics leaders reported that the EOSD management solution enabled the organization to accelerate the amount of time until organizational value was demonstrated. In addition, while not surveyed systematically, improved clinician experience/satisfaction was reported anecdotally to IT leadership and line staff. In particular, the solution helped IT/informatics ensure mobile device availability when clinicians needed one, reducing user frustration that can contribute to clinician dissatisfaction. Leaders noted that the solution not only enabled a consistent user experience with little friction, but also strengthened security by allowing clinicians to access devices rapidly and easily. Clinicians are able to obtain an iPhone with the same identity badge tap already used in workstation single sign-on. This reportedly eased and expedited clinician adoption of the new EOSD management solution. Clinicians' devices are customized/personalized automatically. IT/informatics leaders were satisfied that devices are wiped clean automatically between uses to prevent inappropriate access to PHI, ensuring HIPAA compliance, information security and confidentiality.

4.6 Future expanded utility and value growth potential

Moving forward, the YNHHS IT/informatics team will further deploy the EOSD management solution to enable single sign-on on mobile devices that are shared and to expand usage of its mobile platform. This will further reduce clinician time spent authenticating into various applications. A near term objective is to include more setup profiles on shared devices so that each particular clinician can access and visualize his or her respective high use applications. This enhanced personalization of mobile devices for clinicians is expected to save more time in accessing key functionality, which is freed up for patient care and other activities. In addition, this will enable multiple frequently used platforms, applications, and tool sets that currently exist only on immobile clinical workstations to be migrated to mobile access. YNHHS is also examining the potential introduction of Android devices into its mobility ecosystem, leveraging its new EOSD management solution.

Future improvements in consistency, ease and speed of navigating IT systems will be sought to minimize clinician frustrations and to increase clinician adoption and satisfaction, and hopefully, contribute to ameliorating staff IT burnout. As the number, nature and complexity of mobile devices increases in future years, the imperative to unify management of access policy and ensure effortless clinician workflows across devices will grow, and YNHHS leaders expect the EOSD management solution to position them well for the challenges ahead.

Finally, IT leaders noted the additive or synergistic value that was conveyed by the EOSD management implementation because it was an integral component of the YNHHS Imprivata identity and access management ecosystem. It was stated that this eased/expedited EOSD solution implementation and clinician adoption, but also promises further synergies and an expansion of what YNHHS regards as not merely a customer services relationship with the provider (Imprivata), but an effective partnership that cuts across multiple areas of critical capabilities, functionality, and platform integration presently, and in the future.

5. DISCUSSION

The needs of HDOs with respect to effective management of mobility are diverse and complex, including demonstrated ability to leverage mobile tools to increase care efficiency and reduce clinician friction, fatigue, and professional burnout as contributed to by information technologies. Clinical mobility increasingly requires EOSD management solutions that reduce costs, facilitate access security and interoperability, while also improving security and workflow flexibility.

Effective mobile programs require solutions that reduce administrative burden and create a seamless user experience that streamlines access and device management. A leading US health system was able to deploy a mobile manage-

ment solution that was cohesive and comprehensive, rapidly deployed, and enabled effective monitoring and dynamic management of the enterprise mobile device fleet. EOSD management solutions must also enable better IT resource management and reduced mobile device loss. This use case illustration of the implementation of a systematic mobile strategy and program at Yale New Haven Health System may be instructive to other health systems in pursuing the same objectives and in meeting similar organizational and technology needs.

It was not part of the design of this study to evaluate the impact of an EOSD management solution on several key potential outcomes, including whether the implementation and heightened accountability associated with more robust and rapid device tracking influenced clinician user device monitoring or protective/loss prevention behaviors. In addition, we did not survey systematically to assess for possible improvements resulting in clinician user experience and satisfaction, nor whether time freed up for clinicians in their device management workflow, as well as improved bedside mobile access to patient data for rounding and other care activities, could have a favorable impact on quality of care. These questions would constitute valuable areas of future research on the impact of improved clinical mobility and EOSD management in healthcare delivery organizations. The likely reality is that mobile use in care provision and clinical workflows will increase in the coming years, and understanding these dynamics will be useful in maximizing the effectiveness and efficiency of advanced mobile implementation and refinement.

6. Conclusions

In this clinical mobility use case from the Yale New Haven Health System, clinical workflows and clinician efficiency improved, IT administrative burden was eased, and a meaningful return on investment was realized. System leaders appreciated the rapid time to demonstrated value. Improved clinician user experience and satisfaction were also reported anecdotally to IT leaders and staff. While the complexities associated with increased mobility in healthcare will likely continue to grow, issuing future device and mobile management challenges that demand effective HDO response, solutions such as that described have emerged that enable more effective, efficient, and satisfactory organizational mobility performance.

Acknowledgements

The authors are indebted to the YNHHS IT/informatics team for their support during implementation of the new shared mobile management solution, and to the clinicians that adopted the new processes and conveyed feedback on system performance and needs.

Authors contributions

GAG and SPK led the conceptualization of the study, gathered and integrated the data; GAG wrote the first and subsequent drafts, created the tables, and completed revisions and editing of all drafts; GS, MP, MR and RH provided the data, reviewed and validated the data integration and presentation, and reviewed and approved all drafts of the manuscript; SPK reviewed and provided edits to all manuscript drafts, and supervised the project.

Ethical statement

Informed patient consent was not required because no patient clinical or identity data was collected, and no patient interventions were completed during the course of study. Therefore ethical review board approval was not required and waived.

Funding

This work had no external financial support.

Conflicts of Interest Disclosure

GAG is an external medical advisor to Imprivata; GS, MP, MR and RH are employees of Yale New Haven Health System; SPK is an employee of Imprivata.

Ethics approval

The Publication Ethics Committee of the Sciedu Press. The journal's policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

Open access

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/).

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

REFERENCES

[1] Lee M, Bin Mahmood ABS, Lee ES, Smith HE, Tudor Car L. Smartphone and mobile app use among physicians in clinical practice: Scoping review. JMIR Mhealth Uhealth. 2023; 11: e44765. PMid: 37000498. https://doi.org/10.2196/44765

[2] Juniper Research. Smart hospitals to deploy over 7 million Internet of medical things. 2022. Available from: juniperresearch.com

[3] JAMF. 2018 Survey: The impact of mobile devices on hospital patient satisfaction. Available from: https://www.jamf.com/resources/e-books/2018-survey-the-impact-of-mobile-devices-on-hospital-patient-satisfaction/

[4] American Nursing Association. COVID-19 impact assessment survey - the second year; 2024. Available from: nursingworld.org

[5] Sharma S, Kumari B, Ali A, et al. Mobile technology: A tool for healthcare and a boon in pandemic. J Family Med Prim Care. 2022; 11(1): 37-43. PMid: 35309626. https://doi.org/10.4103/jfmpc.jfmpc_1114_21

[6] US Health and Human Services, Security standards: Physical safeguards. HIPAA Security Series. Security Physical Safeguards. 2007. Available from: https://www.hhs.gov

[7] Jennings A. Hidden costs of missing medical equipment. Chief Healthcare Executive. Hidden costs of missing medical equipment | Viewpoint. 2023; Aug 28. Available from: chiefhealthcareexecutive.com