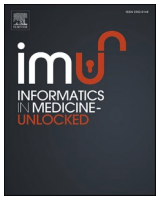
Informatics in Medicine Unlocked 52 (2025) 101603

Contents lists available at ScienceDirect

Informatics in Medicine Unlocked

journal homepage: www.elsevier.com/locate/imu



The love-hate state of mobile device management in healthcare: An international survey

George A. Gellert *, Gabriel L. Gellert, Rachel Pickering, Sean P. Kelly

Imprivata, USA

ARTICLE INFO

Keywords:
Clinical mobility management
Clinical mobility
Mobile device management
Enterprise-owned shared mobile devices

ABSTRACT

Objective: To gather insights regarding mobile device fleet deployment, management and security in healthcare delivery organizations (HDOs), including unmet needs and gaps in capabilities, across four nations.

Methods: An exploratory online survey of health information technology leaders working in HDOs to gather information about respondents' organizational deployment of mobile devices as well as existing and needed mobile management capabilities.

Results: HDO mobile device losses were high, with 42% reporting average annual loss rates of 11–30%. Reported organizational effectiveness in protecting confidential information on lost mobile devices was low, with 50% of respondents ranking at six or below on a 10-point scale. Perception of end user satisfaction accessing applications/data on mobile devices was low, with 56–60% ranking satisfaction at six or below on a 10-point scale. Less than half of HDOs reported seven core mobile device management capabilities. Reported costs of mobile device information security breach across nations were between $100,000 and $1 million (USD). Respondents estimated aggregate weekly downtime exceeds 500h among 28% in Australia, 49% in Germany, 45% in the UK, and 47% in the US.

Conclusions: HDOs reported substantial perceived gaps and challenges in effectively managing mobility. System leaders desire what mobile device workflows add to care delivery, but effectively and efficiently managing a mobile device fleet remains a significant challenge. Mobility management tools are needed to facilitate rapid mobile device authentication, and efficiency of information access, while reducing clinician friction. Existing shared mobile device management solutions can help HDOs reduce costs and improve access security, user experience and workflow flexibility.

1. Introduction

Healthcare delivery organizations (HDOs) are seeking new methods to make point-of-care workflows simpler and more streamlined, and many are engaging mobility projects as enterprise-wide initiatives to improve care effectiveness/efficiency and operational productivity. Growth in the utilization of shared-use mobile devices in healthcare is increasing because they offer greater workflow flexibility, relative cost savings compared to each individual using a unique device, and improved efficiency in accessing information quickly and easily from any location within or outside the principal facility [1]. The expanding Internet of Medical Things (IoMT) is also driving mobile device adoption and optimization, with the number of IoMT devices globally projected to grow 131% by 2026 [2].

By streamlining workflows at the point of care and enabling secure real-time, rapid transfer of patient data across the HDO network, mobile devices offer opportunities to increase clinician workflow efficiency and satisfaction, and have been associated with improved patient satisfaction [3]. Increasing device interoperability has enabled engagement of more clinical workflows at the bedside using mobile device technology, creating greater access to electronic health records (EHRs) and clinical applications at the point of care delivery [4]. HDOs are seeking mobile solutions to improve workflow flexibility and care team collaboration, and which offer budgetary savings and effective human resource management [2]. Mobile devices are less expensive to purchase, manage and maintain than traditional desktop environments, and mobile devices

Abbreviations: HDO, health care delivery organization; EHR, electronic health record; IT, information technology; BYOD, bring your own device; EOSD, enterprise owned shared device; MDM, mobile device management; UK, United Kingdom; US, United States.

* Corresponding author. 703 Sentry Hill, San Antonio, TX, 78260, USA.
E-mail address: ggellert33@gmail.com (G.A. Gellert).

https://doi.org/10.1016/j.imu.2024.101603
Received 7 October 2024; Received in revised form 23 November 2024; Accepted 27 November 2024
Available online 5 December 2024

offer myriad potential applications that can be accessed once properly secured [5].

As a result, growth in clinician use of mobile devices is accelerating [3]). However, accompanying the benefits of mobility are concerns about data privacy and security around proper authentication and efficient management of shared mobile devices as they are exchanged between users. Efficient workflows on mobile devices can be implemented with minimal loss of security or privacy, but remain a challenge. Measures that enhance security can impede usability and adoption, such that HDOs may struggle to optimize mobile investments [4]. Managing digital identity is key to ensuring security and reducing usability barriers, and HDOs must minimize points of mobile device exposure to ensure the highest quality of care delivery with secure mobile access 24/7/365 from any location.

We report an exploratory international survey gathering HDO perceptions on the characteristics of mobile device usage, with a focus on current mobile management capabilities and unmet needs. Little research has been reported on the adoption of mobility by hospitals and care providers, including the demands created by mobile workflows and managing a mobile device fleet, and the challenges HDOs are encountering in their greater use of clinical mobility. While HDOs value the care capabilities and clinician user experience increased mobile workflows convey, lack of standardized adoption processes and practical tools to effectively and efficiently manage mobile device fleets and workflows combine to create a "love-hate" dynamic with a much desired technology that is difficult with existing tools to integrate and manage organizationally. With multinational adoption of clinical mobility and mobile workflows, we suspect that the mobility experiences of HDOs will be more similar than different across the four nations studied.

2. Methods and materials

2.1. Study objectives and hypothesis

This exploratory survey gathered information regarding perceptions and practices of healthcare information technology (IT) leaders on unmet needs in managing clinical mobile devices in their HDOs. Included were unmet needs and challenges in effectively and efficiently managing an enterprise-owned shared device (EOSD) strategy and operations. The objective of this descriptive study was to assess the perceived readiness and capabilities of hospitals in four different nations with respect to emerging mobility management. Our hypothesis is that HDOs will report diverse and substantial issues in adopting mobile devices and workflows, and that many of these will be shared across Australia, Germany, the United Kingdom and the United States.

2.2. Study design and setting

Data was extracted from a December 2023 larger multisector survey of 1795 respondents on mobility in the healthcare, manufacturing, gaming, retail and transportation/logistics industries [6]. A restricted analysis of data from 370 respondents (20.6%) reporting an HDO leadership role and responsibility for deploying and managing use of mobile devices was completed. This included respondents within hospitals and health systems in four nations: Australia, Germany, United Kingdom, and United States. Survey responses were quantified and tabulated.

2.3. Respondent eligibility and selection

An online fully de-identified, anonymous survey sampled respondents from health systems and hospitals. Participation eligibility criteria included respondents having a leadership role in managing mobile device functionality, access, security and distribution at their respective organizations [6].

2.4. Data captured and analyses completed

Survey questions gathered information about respondents' organizational role, care delivery setting, quantity and use level of HDO mobile devices, existing and needed capabilities to manage an EOSD or bring your own device (BYOD) fleet, applications accessed through mobile devices, impact on IT services and users when their mobile device is missing, and perceived organizational benefits of mobile device use. Survey data was analyzed by stratifying nation responses to generate tables evaluating key variables for understanding the current status, needs, gaps and challenges of mobile device use and fleet management. Bar charts were generated to share the results stratified by nation.

3. Results

3.1. Survey completion rate and respondent profile

Total number of HDO survey respondents was 411 with 41 surveys rejected, a survey completion rate of 90.0% of eligible respondents (N=370). Respondent titles included: 18% chief information officer (CIO), 12% chief information security officer (CISO), 16% chief medical information officer (CMIO) or chief nursing information officer (CNIO); and 43% either vice president, director or manager of IT or IT security. Mobile device, network or system administrators comprised 20% of respondents. By nationality, 13% of respondents were from Australia, 32% from Germany, 21% from the UK and 34% from the US.

3.2. Multisector organizational mobile device deployment by nation

Regarding mobile devices provided to users, 41% of organizations deployed enterprise-owned, not shared devices, 32% deployed EOSDs, and 27% had combined deployment. Overall number of mobile devices deployed across nations was: 4% less than 1,000, 17% from 1001–5000 devices, 13% from 5001–10,000, 21% from 10,001–50,000, 25% from 50,001–100,000, and 20% more than 100,000 devices. Deployed mobile devices by nation are shown in Fig. 1. US and German respondents had the highest number of devices with 80% and 73%, respectively, indicating their organization had greater than 50,000 devices.

3.3. Agent responsible for organizational mobile device management strategy

Leadership roles responsible for HDO mobile device management (MDM) were the CIO (29%), CTO (28%), CISO (8%), and chief financial officer (CFO) among 8%. In 21% of HDOs there was no single organizational owner and MDM was a shared responsibility.

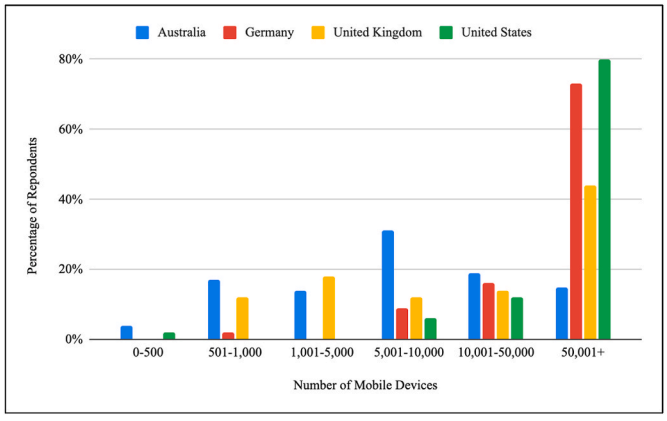


Fig. 1. Number of deployed mobile devices in multisector respondent organizations by nation.

3.4. Annual mobile device loss rate

The highest annual mobile device loss rates were reported in Australia and the United States (Fig. 2). Only 15% of respondent organizations on average reported an annual device loss rate of less than 5%. On average, about one quarter reported annual fleet losses of 5–10%, 29% reported 11–20%, 23% reported 21–30% and 10% reported 31–40%. Fig. 2 is remarkable for the minimal inter-nation variation in yearly device loss rate, mostly clustering in the 5–30% range across all four nations.

3.5. Mobile device replacement cost

Regarding average replacement cost for a single mobile device, 18% on average reported a replacement cost of USD $100–500, 29% reported $501–750, 34% reported $751-1,250, and 19% reported greater than $1,250 (Fig. 3). Most frequently reported mean replacement cost per device was $751-1,250 (34% of respondents), followed by $501–750 (29%). Almost one-fifth (19%) of respondents across nations indicated a replacement cost exceeding $1,250. Nations with highest device replacement costs in excess of $750 were Germany (58%) and the United Kingdom (56%). Little variation by nation in the breakdown of replacement cost is evident.

3.6. Organizational effectiveness in protecting confidential information on lost mobile devices

Respondents ranked on a 10-point scale their HDO effectiveness protecting confidential information on lost mobile devices, where 10 was maximum effectiveness (Fig. 4). Effectiveness at six or below was reported in about 50% of responses, indicating considerable concern among many respondents across nations about essential confidential data protection capabilities of their HDO.

3.7. Ease of access to applications/data on shared mobile devices

With respect to ease of access to applications and data on shared mobile devices, a majority of respondents across nations ranked user ease between 3-6 on a 10-point scale. There was relatively little inter-nation variation reported in ease of user access to applications and data on mobile devices, with most nations within 2–4% of each other (Fig. 5).

3.8. Organizational effectiveness in controlling access to mobile device applications and confidential data

Respondents had low confidence in their organizational effectiveness in controlling access to applications, with 55% on average rating effectiveness between 1-6 on a 10-point scale (Fig. 6). UK and US respondents appeared more confident in this regard than Australian and German counterparts.

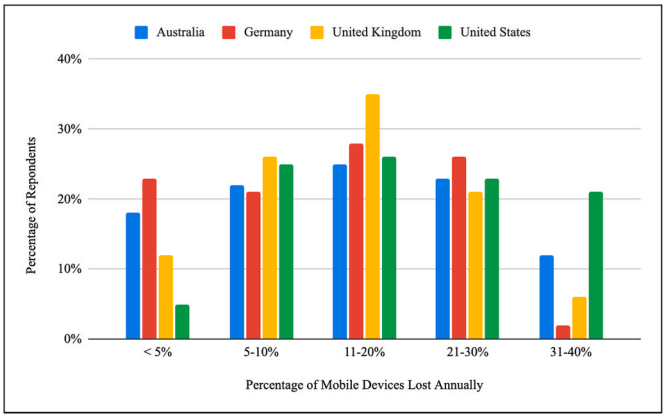


Fig. 2. Percentage of mobile devices lost annually.

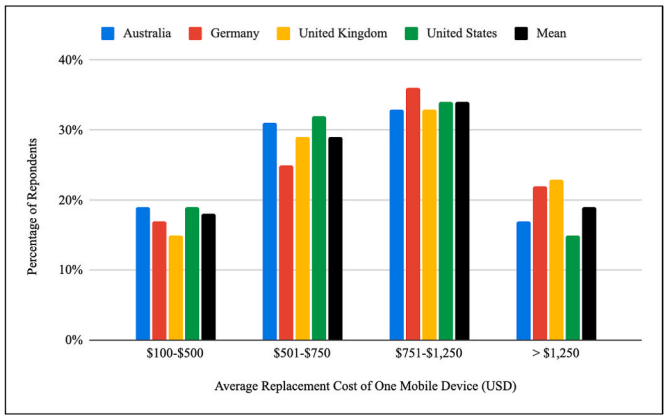


Fig. 3. Mean replacement cost per mobile device.

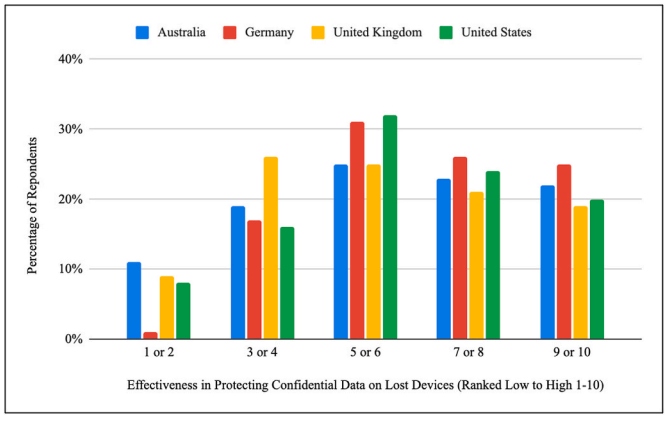


Fig. 4. Organizational effectiveness in protecting confidential data on lost mobile devices.

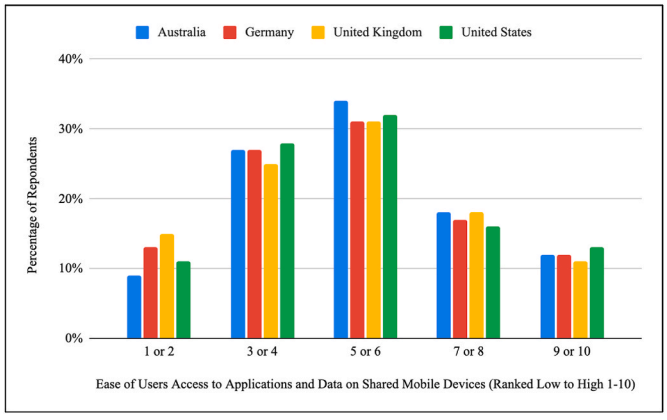


Fig. 5. User ease of access to applications and data on shared mobile devices.

3.9. Clinical user satisfaction with mobile device access to applications and data

Perceptions of clinician satisfaction with accessing applications/data on mobile devices showed little variation (4-5%) by nation, with 56–60% of respondents ranking satisfaction at six or below on a 10-point

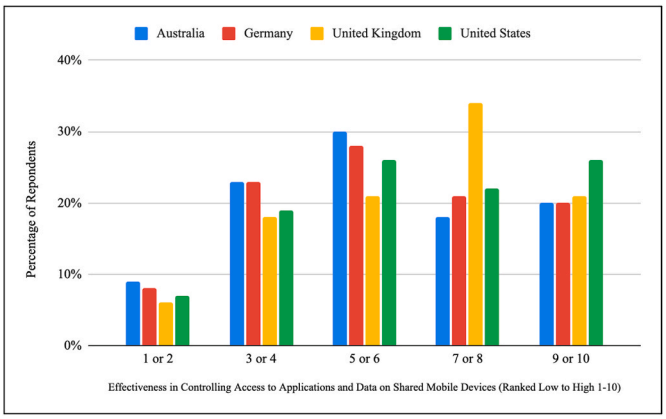


Fig. 6. Organizational effectiveness in controlling access to applications and confidential data on shared mobile devices.

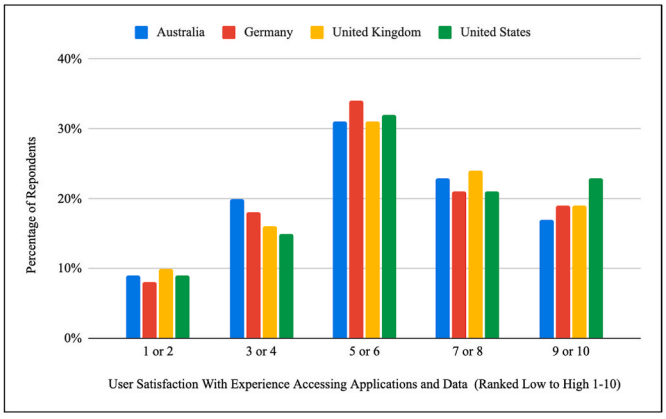


Fig. 7. Clinical end user satisfaction accessing applications and data on mobile devices.

scale (Fig. 7).

3.10. Current mobile device management capabilities

Respondents ranked current core capabilities within their organization's MDM program. Across the four nations, over one-fourth indicated their HDO had implemented none of the capabilities assessed (Fig. 8). On none of the core mobile management capabilities did 60% or greater of respondents report existing implementation.

3.11. Key mobile device management requirements

Regarding key MDM objectives and requirements, 30–42% of respondents stated they had none (Fig. 9). Roughly one-half or less of HDOs reported instituting any of seven basic or essential MDM requirements.

3.12. Organizational measures to manage mobile device data accessibility

Asked about existing organizational measures to manage user mobile device accessibility to data, respondent minorities indicated their HDOs had key measures in place (Fig. 10). A majority of respondents stated that measures to manage data accessibility on mobile devices were not automated, and involved manual policies, audits and standard operating procedures. Almost half of respondents across nations stated their organizations had no password enforcement, remote lock or wipe of devices, containerization or application wrapping.

3.13. Organizational measures to secure data accessible on enterprise-owned mobile devices

Respondents indicated higher levels of organizational measures in place to secure data accessibility on enterprise-owned mobile devices, however on only a few measures did HDO response exceed 50% (Fig. 11). Almost half reported having no anti-malware, jailbreak/root detection, or device encryption, and over half do not secure data in transit or within vulnerable applications.

3.14. Cost to detect, contain and remediate mobile device unauthorized data access or breach

Respondents were asked to estimate the maximum cost of detecting, containing and remediating a breach or unauthorized access to mobile device data. One-third of Australian respondents estimated this value as exceeding $1 million, as did 31% of respondents in Germany, 23% in the UK and 40% in the US. The most frequently reported cost range across nations was $100,000-$1 million (Fig. 12), with 70% of respondents indicating the cost of mobile device data breaches exceeded $250,000 per episode.

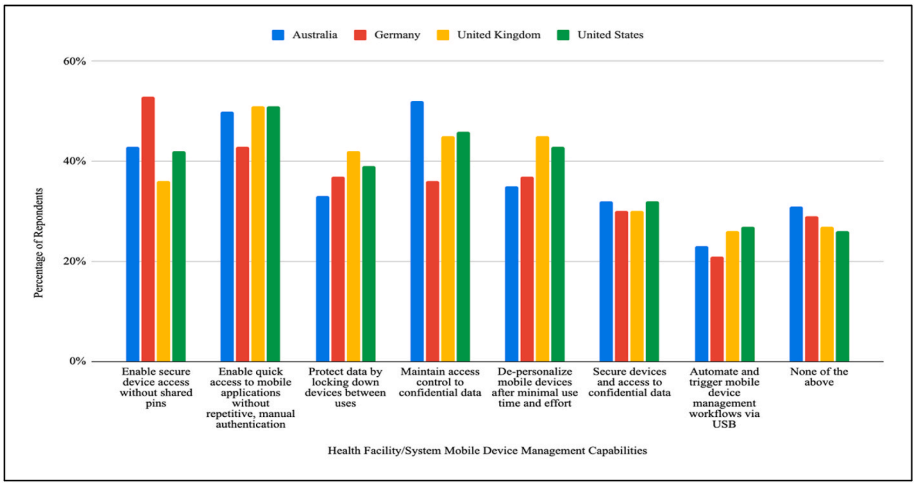


Fig. 8. Capabilities of current organizational mobile device management program.

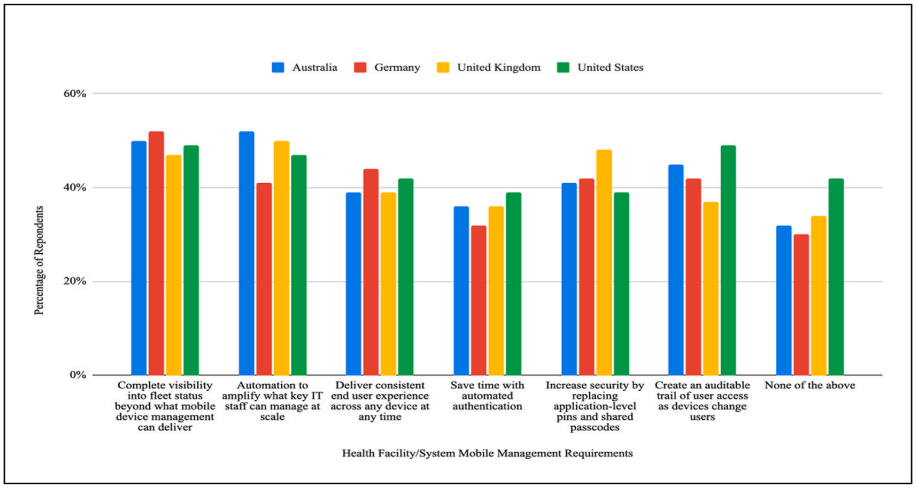


Fig. 9. Health facility/system mobile management objectives and requirements.

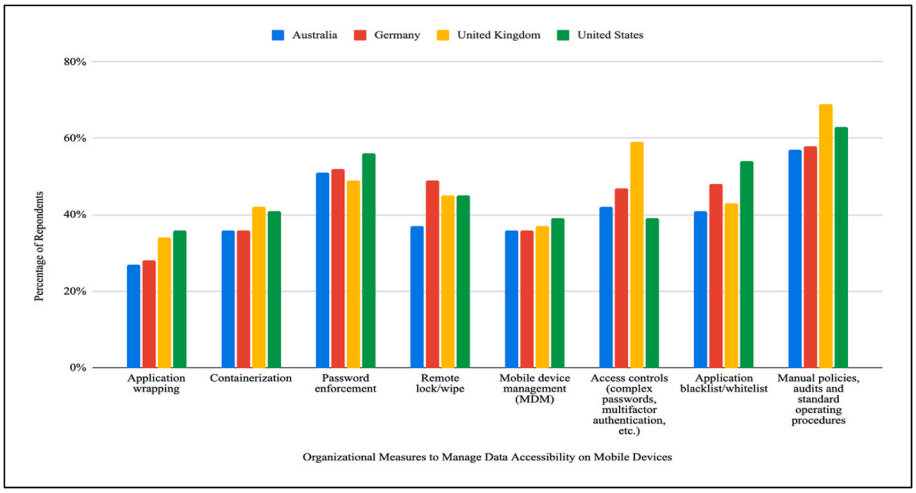


Fig. 10. Organizational measures to manage data accessibility on mobile devices.

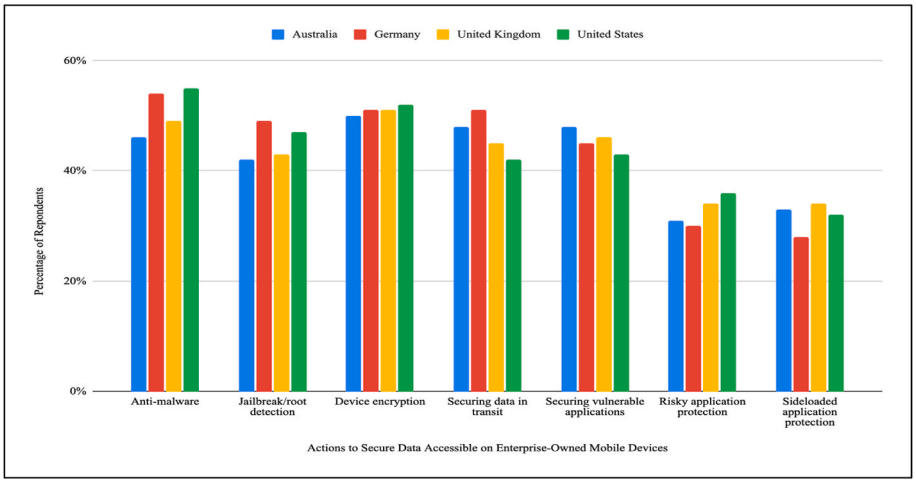


Fig. 11. Organizational measures to secure data accessible on enterprise-owned mobile devices.

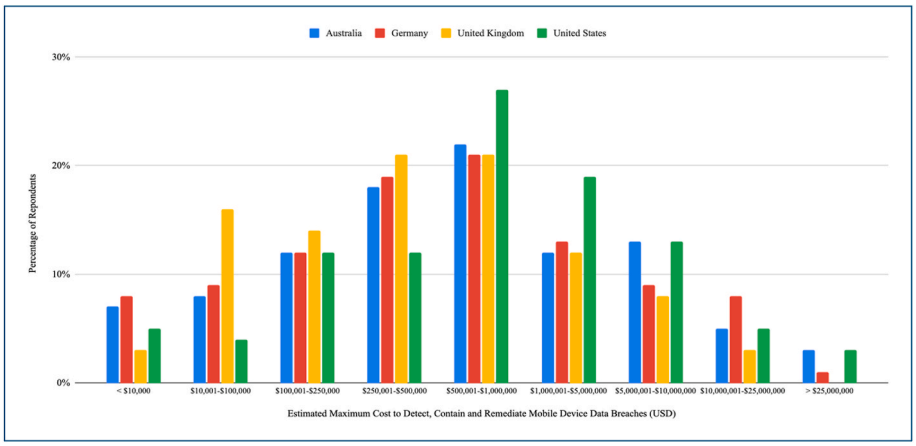


Fig. 12. Estimated maximum cost to detect, contain and remediate mobile device unauthorized data access or breach.

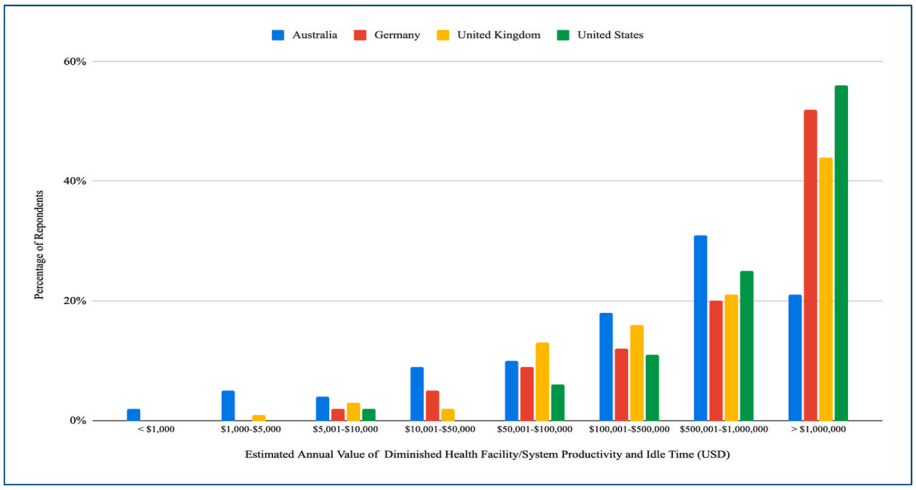


Fig. 13. Estimated annual value of health facility/system diminished workforce productivity and idle time.

3.15. Estimated annual value of health facility/system diminished workforce productivity and idle time

The highest estimated value of lost productivity was reported in the US, with 81% of respondents indicating in excess of $500,000/year, followed by Germany (72%), the UK (65%) and Australia (52%) (Fig. 13). Total cost of productivity loss and idle time was substantial across nations, with less than a fifth of respondents indicating it is below $100,000 per annum.

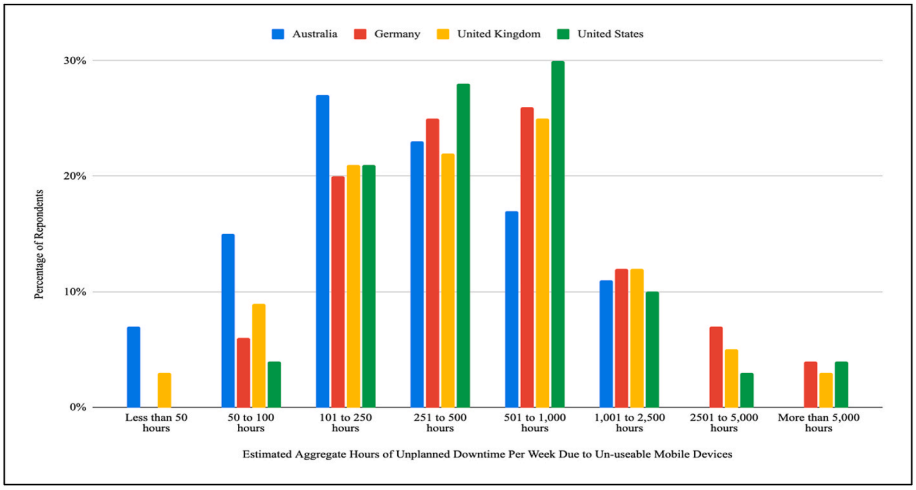


Fig. 14. Estimated aggregate hours of unplanned user downtime per week due to non-functional mobile devices.

3.16. Estimated aggregate hours of unplanned user downtime per week due to non-functional mobile devices

Fig. 14 shows respondents' estimates of aggregate hours per week of unplanned clinician downtime due to non-functional mobile devices. Striking are the German and UK estimates, where 23% and 20% of respondents, respectively, indicated that downtime exceeded 1,000 total hours per week, with only the US reporting a greater level. Australian respondents estimated unplanned downtime durations considerably less than other nations. A majority of HDO respondents across nations reported total estimated unplanned downtime exceeding 100h per week. Fewer than 20% indicated total weekly time lost less than 100h or greater than 2500h across the organization.

4. Discussion

4.1. The findings: Clear need for improved mobile management capabilities

The survey data suggests that for many HDOs, effectively and efficiently managing mobile devices remains a challenge and aspiration yet to be realized. Across these four nations, respondents reported similar degrees of inferior, incomplete or absent core capabilities for managing a mobile device fleet in a manner that maximizes cybersecurity and ease of use for clinicians and IT staff, while reducing risk of unauthorized access and costly annual device losses. The findings demonstrate compellingly that HDOs recognize the value and need for mobile devices and for effective fleet management, but are unsatisfied with current capabilities to do so. In many gap areas and concerning most issues, the magnitude of differences between respondents from the four nations surveyed was small.

Mobile device loss is a major problem across all four nations, with respondent majorities reporting more than 10% annual loss rates, and higher in Australia and the US. The cost of annual mobile device loss is not insignificant, with about one-fifth of respondent organizations paying in excess of US $1,250 per device replaced, and majorities paying more than $750.

With respect to perceived organizational effectiveness in protecting confidential data on lost mobile devices, the findings are sobering: a majority of respondents ranked their effectiveness at six or below on a 10-point scale. Little inter-nation variation was observed. Perceived organizational difficulty in maintaining access controls on shared mobile devices was high, with a majority across nations ranking difficulty at seven or higher on a 10-point scale, and one-third ranking difficulty as very high (at 9–10).

Respondents had little confidence in the ease of user access to applications and data on shared mobile devices, with less than 30% ranking this at 7–8 or greater on a 10-point scale, and minor variation between nations. Perceived organizational effectiveness in controlling access to applications and confidential data on shared mobile devices was also low and ranked at 5–6. Similar ranking was reported for user experience and satisfaction in accessing applications and data on mobile devices, with a majority across nations ranking at 5–6 or below on a 10-point scale. Overall, the clustering and lack of variance of views, status and experience across the four nations is impressive.

The aspirational status of most HDOs regarding core MDM capabilities was well illustrated: for seven basic capabilities, low majorities indicated they had only a single capability (namely to quickly access mobile applications without repetitive, manual authentication). In few of the other critical functionalities did a majority of respondents in any nation indicate an existing capability, with two exceptions: Australian respondents indicated an existing ability to maintain access control to confidential data, and German respondents access to mobile devices without use of shared pins. Remarkably, over one-quarter of respondents across nations indicated they had none of seven basic mobile management capabilities. Further, when asked about six basic health system objectives for MDM, across nations majorities indicated they did not have these core organizational requirements.

Across eight critical measures to manage mobile device data accessibility, a majority had implemented only half (password enforcement, access controls such as multifactor authentication, application blacklist/whitelist, and manual policies, audits and standard operating procedures). On only two of seven (anti-malware and device encryption) did slight majorities confirm implemented measures to secure data accessible on enterprise-owned mobile devices. Again, the findings are striking for how little inter-nation response variation exists.

Yet in all nations a majority of respondents indicated that the costs of detecting, containing and remediating unauthorized data access to mobile devices are substantial and in excess of USD $500,000 per year. Costs were highest in the US, with 40% of HDOs reporting they exceed $1 million per year, compared to 33% in Australia, 31% in Germany and 23% in the UK. Annual costs exceeding $5 million were reported by 21% of Australian, 18% of German, 11% of UK and 21% of US HDOs. It is unclear why these costs are lower in the UK.

Thus, lack of effective mobile management capabilities is a significant source of avoidable cost and waste across nations. Estimated annual decreases in workforce productivity and increased clinical and administrative staff idle time were impressive. Across all four nations this exceeded $500,000 per year, and in Germany and the US exceeded $1 million in lost productivity annually. Most respondents estimated the aggregate hours of unplanned user downtime per week as 251-1,000h.

As a web-based survey, these analyses have the usual methodological limitations of non-response bias and sampling frame bias, as well as potential quality limitations related to self-reported data.

4.2. Way forward: Technological solutions for technology induced challenges

In recent years technology solutions have emerged to effectively and efficiently manage a mobile device fleet and support a secure, consistent workflow experience in accessing applications and clinical information. For example, when Yale New Haven Health System (YNHHS) sought a mobile management capability set with shared device workflows, Imprivata Mobile Access Management was selected as an EOSD management solution. This technology platform was used to automate smartphone provisioning, and to provide a comprehensive access control solution that would streamline mobile device access and authentication [4]. Cloud-based management tools enabled tracking, support and maintenance of mobile devices. Mobile Access Management was integrated with the existing, earlier implemented Enterprise Access Management single sign-on solution, which enabled a rapid, familiar and consistent authentication process for clinicians on clinical workstations, virtual desktops and mobile phones. Clinicians readily adopted the new EOSD management solution because it leveraged secure access technology and workflows they were already using and familiar with to access clinical workstations, the health system EHR, and other clinical applications [4].

YNHHS IT administrators established user authentication policies across information systems and diverse workflows from a centralized platform, which improved reporting compliance and reduced total cost of ownership [4]. IT resources expended in managing authentication workflows decreased, as did annual mobile device loss. Users accessed shared mobile devices with a proximity identity badge tap that enabled rapid access to applications, and eliminated need for manual authentication. The cloud-based EOSD management platform is updateable from any location at any time, with personalized device checkout and easy application access. For physicians accessing PHI from a BYOD personal device, Imprivata Confirm ID improved security by enabling enterprise-wide two factor authentication for remote network access, cloud applications, and Windows servers and desktops [4]. Imprivata Enterprise Access Management was also deployed for electronic prescription of controlled substances, to provide the broadest range of US

Drug Enforcement Agency compliant two-factor authentication modalities, including hands free authentication, push token notification, and fingerprint biometrics that are fast and convenient for providers [4].

YNHHS derived multiple benefits from the implementation of this solution, which conveyed a cohesive and comprehensive enterprise-owned, shared device management strategy and capabilities set. Reported clinician user experience and satisfaction improved, along with the ease and effectiveness of mobile workflows, mobile device monitoring and IT department management of the system's mobile device fleet [4]. Yale achieved better IT resource management and reduced mobile device loss and associated costs. IT administrative burden was reduced and a clear return on investment and demonstration of value were achieved rapidly [4].

5. Conclusions

Our findings confirm the study hypothesis that HDOs need diverse and complex capabilities to effectively manage mobile tools and workflows, and perceived gaps and challenges are largely consistent and shared across the four nations evaluated. At this stage of evolution, clinical mobility presents HDOs with a love-hate dynamic: clinicians and health system leaders much appreciate and desire what mobility adds to the delivery of care, productivity and clinician experience, but effectively and efficiently managing this powerful technology presents numerous challenges and complexities. This was consistently the case among HDOs across the four nations studied. Mobility management tools are needed to facilitate rapid, efficient and easy mobile device authentication and information access, while reducing clinician friction. Existing EOSD management solutions can help HDOs reduce costs, and improve access security and interoperability, user experience and workflow flexibility. Effective MDM requires solutions that reduce administrative burden and create a seamless user experience that streamlines access and device management.

Mobility is a powerful evolution in the health information technology ecosystem, enabling clinicians to bring the EHR and associated clinical informatics platforms and tools to the bedside, opportuning more patient-centric care. Clinical mobility will soon become a new operating standard in global medicine. Effectively managed mobility may also potentially reduce clinician EHR and information technology professional burnout by expediting workflows and increasing care efficiency, while also improving patient experience and satisfaction from more physician bedside time. Technology solutions have been designed to help HDOs achieve these objectives, and to overcome the challenges evaluated in this multinational survey. Such solutions, enabling the foundational and critical elements of an effective MDM strategy, will advance the HDO health IT ecosystem and patient-centered care delivery, while reducing resources lost through missing devices and time wasted in associated technology downtime and work idles.

CRediT authorship contribution statement

George A. Gellert: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Project administration, Investigation, Formal analysis, Conceptualization. **Gabriel L. Gellert:** Writing – review & editing, Writing – original draft, Visualization, Project administration, Formal analysis, Data curation. **Rachel Pickering:** Writing – review & editing, Methodology, Conceptualization. **Sean P. Kelly:** Writing – review & editing, Project administration, Conceptualization.

Institutional review board approval

This study did not involve patient data, and the survey was completed on a opt-in basis where respondents agreed to have their data analyzed and published in aggregate, de-identified form. As such, a waiver of IRB ethical approval was granted.

Ethical statement

All data was collected observing strict data confidentiality, privacy and ethical research standards. All respondents opted in to survey participation and accepted the survey terms that declared their individual data would be analyzed and presented in aggregate form and in a fully de-identified manner. No personally identifiable information from individuals or companies was collected. As a result, ethical board review was waived.

Funding

This study was not supported by external funding.

Declaration of competing interest

GAG and GLG are external investigators and advisors to Imprivata; RP and SPK are employees of Imprivata.

Acknowledgements

The authors acknowledge the contributions of L. Ponemon PhD and S. Jayson MBA of the Ponemon Institute, who co-designed the survey with Imprivata, implemented the cross-sector survey and collaborated in generating the data. The Ponemon Institute conducts research on issues affecting the management and security of sensitive personal and organizational information that advances responsible information management practices within industry and government.

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. J Med Internet Res Mhealth Uhealth 2023;11:e44765. https://doi.org/10.2196/44765. PMid: 37000498. [Accessed 23 November 2024].

[2] Juniper Research. Smart hospitals to deploy over 7 million Internet of medical things. January. Smart hospitals to deploy over 7 million Internet of medical Things. Press; 2022. [Accessed 23 November 2024].

[3] JAMF (Just Apple's Management Framework). Survey: The impact of mobile devices on hospital patient satisfaction. 2018 survey: The impact of mobile devices on hospital patient satisfaction. JAMF 2018 [Accessed 23 November 2024].

[4] Gellert GA, Stanton G, Paulemon M, Roberts M, Hardcastle R, Kelly SP. Challenges and opportunities in achieving secure hospital mobility management: An illustrative use case. J Hosp Adm 2024;13:1–9. https://doi.org/10.5430/jha.v13n2p1 [Accessed 23 November 2024].

[5] Jennings A. Hidden costs of missing medical equipment. Chief Healthcare Executive. Viewpoint. 2023; Aug 28. https://www.chiefhealthcareexecutive.com/view/hidden-costs-of-missing-medical-equipment-viewpoint [Accessed 23 November 2024].

[6] Ponemon Institute. Unlocking the cost of chaos: The state of enterprise mobility in life-and mission-critical industries. 2024 Ponemon report. Imprivata; March 2024. [Accessed 23 November 2024].