Semi-systematic review

Bring-your-own-device in medical schools and healthcare facilities: A review of the literature

Corresponding author
Khutsafalo Kadimo
BLIS
Department of Library Services
University of Botswana
4775 Notwane Rd.
Private Bag UB 0022
Gaborone, Botswana
khutsafalo.kadimo@mopipi.ub.bw or kkadimo@gmail.com
Telephone: +267 355 5606 or +267 74 258 403

Co-authors
Masego B. Kebaetse, PhD, Department of Medical Education, University of Botswana, Gaborone, Botswana

Dineo Ketshogileng, MLIS, Department of Library Services, University of Botswana, Gaborone, Botswana

Lovie Edwin Seru, PhD, Communication and Study Skills Unit, University of Botswana, Gaborone, Botswana

Kagiso B. Sebina, BSc, Botswana-University of Maryland School of Medicine Health Initiative, Gaborone, Botswana

Carrie Kovarik, MD, Department of Dermatology, Dermatopathology, and Infectious Diseases, University of Pennsylvania, Philadelphia, PA, USA

Kutlo Balotlegi, BSc (honors), Department of Medical Education, University of Botswana, Gaborone, Botswana
ABSTRACT

Background: The ‘culture’ or ‘habit’ of using personal mobile devices for work and learning is expected to continue growing with advances in information and communication and network technologies. Even with the benefits of users bringing their personal devices to working and learning spaces, the fluid relationship and user movement between medical schools and healthcare facilities can pose challenges for data security, particularly patient information security. The bring-your-own device (BYOD) policy is perceived as a driver for balancing user needs for convenience and institutional needs for security.

Objective: This review sought to explore the literature to identify BYOD policy components (issues, interventions, and guidelines) that could potentially inform BYOD policy development and implementation in healthcare facilities and medical schools.

Methods: A literature search on PubMed, Web of Science, and Ebscohost (Academic Search Premier, ERIC, CINAHL, and MEDLINE) was conducted using the following search terms and their synonyms: healthcare facilities, mobile devices, BYOD, privacy and confidentiality, and health records. We developed a review matrix to capture the main aspects of each article and coded the matrix for emerging themes. The database and hand search yielded 1,594 articles, 14 of which were deemed as meeting the inclusion criteria.

Results: Themes emerging from the study include: device management, data security, medical applications, information technology, education and/or curriculum, policy, and guidelines. The guidelines theme seems to provide a direction for BYOD policy development and implementation.

Conclusion: A more feasible approach towards achieving a safe mobile device use environment is through the development of comprehensive BYOD policies that would balance users’ need for convenience with organizational security and patient privacy. The paucity in peer-reviewed literature calls for robust research that uses socio-technical
approaches to development and evaluation of BYOD policies in healthcare facilities and medical schools.

**Keywords:** Bring-your-own-device (BYOD), mobile devices, mhealth, mlearning, medical education, healthcare facilities
INTRODUCTION

While bring-your-own-device (BYOD) is generally conceptualized as the use of personal mobile devices [1-7], Disterer and Kleiner [5] argue that BYOD is the policy that enables the use of personal mobile devices; that is, mobile devices or their use do not in themselves constitute BYOD until there is an associated policy (a plan for achieving set goals [8]). The BYOD policy would therefore be a plan for leveraging the benefits of mobile device use by fostering a safe and appropriate mobile device use environment [9]. Concerted efforts are required to establish and enforce policies that would balance the integration of both information and communication technologies (ICTs) and information use factors to guide the implementation of BYOD [8].

Enabling personal mobile device use through a BYOD policy can potentially save medical schools and healthcare facilities huge amounts of money, as they would not have to acquire facility-owned devices [4,7,9,10]. In addition, employees would be more efficient when working with their personal mobile devices. This would inevitably improve productivity and customer satisfaction [4,7,9,10] through the enhancement of communication and patient care [4,7,9-11]. Furthermore, personal mobile device use can potentially provide for convenient access, retrieval, storage, and sharing of information [6,12,13] in preferred formats [1] and sometimes without the Internet by both students and employees [15].

Enabling BYOD can also precipitate challenges such as unsecure [16-21] and inappropriate use of mobile devices, [7,9,16,18,21,22] including medical applications (apps) [10]. These challenges are in most cases attributable to lack of technologies and systems for managing communication [16,23,24], network controls [7,10], and education [4,17,18,25]. Nonetheless, the lack of guidance in the form of BYOD policies [20,26,27] or mobile device use policies
and regulations [25] remains a challenge for medical schools and healthcare facilities; hence a strong suggestion for enactment of policies as measures for ensuring effective BYOD implementation [16,23,28,29]. However, there seems to be a paucity in the literature on BYOD policy development, policy evaluation, and evaluation of mobile device implementation projects [3,30].

This paucity in the literature can potentially contribute to the lack of guidance in developing, implementing, studying, and evaluating BYOD policies. However, although dispersed, the literature seems to highlight possible components of BYOD policies that could potentially form the basis of comprehensive BYOD policy development. In this review, therefore, we explored the literature to identify BYOD policy components (issues, interventions, and guidelines) that could potentially inform BYOD policy development and implementation in healthcare facilities and medical schools.

METHODS

Study background

As part of our mlearning initiative, we initially provided institutional devices to students and staff preloaded with learning and point-of-care resources [31-33]. Along the way, we decided to explore BYOD as way to expand and sustain our project beyond the life of the grant that funded our project. Our initial plan was to review the literature on BYOD policies in order to glean ideas that could inform our own BYOD policy formulation. The preliminary search seemed to suggest a paucity in peer-reviewed published literature on BYOD policies. However, some papers addressed possible components of BYOD implementation, particularly issues, interventions, and guidelines that emerged from BYOD environments.
Consequently, we shifted our focus from searching for existing policies to exploring how these various components could potentially inform BYOD policy formulation.

**Methodological overview**

We conducted a semi-systematic thematic review of the literature, combining the methodical nature of systematic reviews for searching and documenting our processes with the inductive and analytic nature of qualitative research to explicate emerging and previously identified themes [34-36]. We reviewed the literature broadly, identifying what was already known, gaps in knowledge, and what still needed to be considered [36], and sought to derive a ‘conceptual contribution’ from the literature [34]. To enhance methodological rigor, we paid attention to the principles of qualitative research by clarifying the purpose of the review, collaborating, engaging in purposeful sampling, and considering alternative perspectives [35]. This review, therefore, is intended to expand on current understanding of BYOD implementation [35].

**Data searching and ‘mining’**

A search and ‘mining’ of the literature was conducted between July and August 2016. A predetermined search strategy was used to search PubMed, Web of Science, and Ebscohost (Academic Search Premier, ERIC, CINAHL, and MEDLINE) using the following basic keywords and their synonyms: mobile devices, cell phones, bring-your-own-device (BYOD), medical schools, medical student, healthcare facilities, and healthcare professionals (see Table 1). The search strategy was based on prior search results. Even though BYOD is linked to recent rapid growth and improvement in mobile communication computing technologies, a time period was not used as a search filter to allow the review to be as inclusive as possible.
Table 1: Search strategy for BYOD in healthcare facilities and medical schools

<table>
<thead>
<tr>
<th>Keywords</th>
<th>Synonyms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile device*</td>
<td>Wireless technolog*, instrumentation*, handheld device*, hand-held device*</td>
</tr>
<tr>
<td>Cell phone*</td>
<td>Cellular phone*, mobile phone*, mobile device*, smartphone*, smart-phone*, tablet, iPad</td>
</tr>
<tr>
<td>Bring-your-own-device (BYOD)</td>
<td>Bring your own phone (BYOP), bring your own technology (BYOT), bring your own personal device</td>
</tr>
<tr>
<td>Medical school*</td>
<td>University, tertiary schools, post-secondary school, colleges, faculty of medicine, medical school*</td>
</tr>
<tr>
<td>Healthcare facilities</td>
<td>Hospital*, clinic*, healthcare center*, healthpost*, health-post*, health post*</td>
</tr>
<tr>
<td>Medical student*</td>
<td>Student doctor*, residents</td>
</tr>
<tr>
<td>Healthcare professional*</td>
<td>Medical doctor*, doctor*</td>
</tr>
<tr>
<td>Policies</td>
<td>Information access polic*, information security polic*, bring-your-own-device polic*, information technology polic*, IT polic*, network polic*, IT support, healthcare polic*, hospital polic*, health* records, patient protection, privacy, confidentiality, patient records, patient information</td>
</tr>
<tr>
<td>Other terms used in refining the search</td>
<td>Risk management, practice management, hospital information systems, telemedicine</td>
</tr>
</tbody>
</table>

The initial search yielded 1,582 articles with an additional 12 articles identified through hand searching, leading to a total of 1,594 articles. Due to the contemporary and fast-evolving nature of BYOD, we included English peer-reviewed journal articles and grey literature such as magazine articles that articulate issues, recommendations, or interventions relating to the use of personal mobile devices. KK reviewed titles and abstracts twice in order to identify relevant articles and this resulted in 125 articles (including hand-searched articles). KK and MBK reviewed titles, abstracts, and in some instances full texts, and this resulted in 19 articles. KK reviewed full texts of all the 19 articles and selected 14 articles meeting the inclusion criteria of the study (see Figure 1).
A review matrix was developed based on preliminary data using the headings author(s), year, country, title, article type, issues, interventions, and guidelines to record the main elements of each of the 14 articles (see Appendix A). Once the review matrix was completed, KK, MBK, and DK reviewed the matrix for completeness and for the purpose of becoming familiar with the data. We conducted open coding to identify salient ideas (codes) such as data encryption and password protection [37,38]. We repeated the process twice to forestall a possibility of missing any salient ideas. We grouped the codes into broad themes, after which we reviewed each theme for sub-themes (see Table 2).
Table 2: Summary of the themes and related studies

<table>
<thead>
<tr>
<th>Theme</th>
<th>Studies: issues</th>
<th>Studies: interventions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encompasses issues and related interventions in the management of physical mobile devices such as digital overload, cross-infection, device theft or loss, mobile device embedded keypads, and mobile device use preferences</td>
<td>[9,16,20-23,25]</td>
<td>[16,22-24,27]</td>
</tr>
<tr>
<td><strong>Data security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encompasses issues and related interventions in the management of data created, accessed, and manipulated by mobile devices such as convenience versus security, patient health information (PHI) storage and transmission, security, password protection, data encryption, antivirus protection, remote data wipe, and device locking</td>
<td>[9,16-22]</td>
<td>[9,16,18,21-25,27]</td>
</tr>
<tr>
<td><strong>Medical apps</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encompasses issues and related interventions for the development and use of mobile device medical apps such as medical app information accuracy, rapid increase of mobile devices overwhelming their regulation, and risk assessment frameworks</td>
<td>[25]</td>
<td>[9,23-25]</td>
</tr>
<tr>
<td><strong>Information technology</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encompasses issues and related interventions that are a responsibility of Information Technology (IT) departments such as network control, hospital communication systems, Wi-Fi, bandwidth, and mobile device compatibility</td>
<td>[9,16,17,23,27]</td>
<td>[9,16,22,24,27]</td>
</tr>
<tr>
<td><strong>Education and or curriculum</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encompasses issues and related interventions in medical education, specifically the curriculum such as medical schools curricula and mobile device use etiquette</td>
<td>[16-19,21,25]</td>
<td>[17,22,23,25]</td>
</tr>
<tr>
<td><strong>Policy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encompasses policy-related issues and interventions that emerge from BYOD and that capacitate healthcare facilities and medical schools environments, such as BYOD policy, IT policy and infrastructure, mobile device use policy, and social media policy</td>
<td>[20,26,27]</td>
<td>[9,16-19,22,23,26,27]</td>
</tr>
<tr>
<td><strong>BYOD guidelines</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encompasses general lessons or recommendations for BYOD that capacitate the management of healthcare, such as lifting bans to guide the use of personal mobile devices, investing in BYOD, optimizing BYOD monetary savings, and providing sufficient clarity about mobile device use-related liabilities</td>
<td>[16,19,21-24,26]</td>
<td></td>
</tr>
</tbody>
</table>

**RESULTS**

The search yielded 1,594 articles, including the 12 hand-searched papers. After de-duplication and iterative review of abstracts and full texts, 14 articles were identified as meeting the inclusion criteria, 8 of which were original research articles [9,17-21,26,39]. Five were magazines articles (all coming from the USA) [16,22-24,27] and one a viewpoint journal article [25]. All the publications were from high-income countries as follows: nine from the USA [9,16,19,20,22-24,27,39], two from the UK [25,26], two from Canada [17,18] and one from Ireland [21]. The identified review articles were published between 2012 and
2016: one in 2012 [20], two in 2013 [23,27], five in 2014 [16,17,21,24,25], two in 2015 [19,22], and four in 2016 [9,18,26,39].

Seven themes emerged from the analysis, namely device management, data security, medical apps, IT, education and/or curriculum, policy, and guidelines, as represented in Figure 2. Device management, data security, medical apps, IT, education and/or curriculum themes are components of BYOD policy. Each component comprised of issues and interventions. The policy theme appeared to be a comprehensive solution that synergizes the other five components. The guidelines theme, on the other hand, appeared to provide direction for BYOD policy development and implementation.

Figure 2: Emerging themes relating to BYOD policy formulation
Device management

This theme encompasses issues and interventions that relate to the management of physical devices. Several issues that are related to device management emerged from the analysis: digital overload [9,16,22,23], preference of unsecured personal devices over secure provisional (institution provided) devices [16,23], preference for keeping personal and work devices separate, cross-infection due to the device being an infectious agent [16,21], and device theft or loss [16,20-23]. Mobile device embedded keypads can lead to issues of poor data entry, while device small screen size can contribute to issues of compromised and complicated data and image viewing [16,23,25].

Interventions for addressing issues that relate to device management include: fostering provisional devices preference [27], registering personal mobile devices for use in the workplace [16,22-24], and controlling sale, trade-ins, and gifting of mobile devices loaded with patient health information [22].

Data security

The data security theme encompasses issues and interventions that relate to the management of data that reside in the mobile device or are accessed through the use of the device. Data security issues include: tendency to choose convenience over security [9,17-21], unsecure PHI storage and transmission [9,16,18,21,22], accessing work e-mail using mobile device and forwarding e-mail with attachments [17,22], privacy breaches due to hackers and virus attacks [16], and lack of enterprise management tools for improving security [16]. Other issues are lack of device password protection, lack of device locking mechanism, lack of device encryption [16-21], lack of antivirus protection [16], lack of remote data wipe [17], and potential loss of personal data [17].
Procedural system management interventions include: two- or three-layer security on data transmission [9,23]; role-based messaging [16]; data encryption [18,21-23]; closed-loop communication [16]; remote data wipe when device is lost, stolen, or changing ownership [9,21,22,27]; safe cloud access or virtual desktop [16,22,24]; and appraisal of each data transfer [24]. Other recommended interventions include: device automatic log-off when inactive [9], password protection [18,21], advanced encryption [22,27], antivirus and malware software protection [22], and prompt reporting of lost or stolen devices [22]. A prohibition of the following activities was also recommended as interventions for data security: file batch downloading, family usage of PHI active devices, storage of PHI in mobile devices [16,25], unsecure text messaging [16], and installation of free apps on PHI mobile devices [22]. Furthermore, there were also recommendations for the regulation of mobile device access to PHI [16], period for device PHI storage [23], copy data, print screen functionality, and cloud services backup [9].

Medical apps

This theme encompasses issues and interventions that arise from the development and use of mobile device medical apps. Issues that relate to mobile device apps include: questionable information accuracy due to developers’ lack of medical background, rapid growth, inadequate or lack of regulation, lack of risk assessment framework [25], limited regulatory support for physicians, and possible poor clinical decision making [25].

Interventions for controlling medical app inaccuracies include: developing regulation models and guidelines, keeping up-to-date lists of recommended medical apps [23], validating medical app captured data, limiting app access to authenticated sources only [25], and
garnering support from medical bodies or associations [25]. App data security interventions include: restricting medical apps to internal or virtual private networks; encrypted password-protected devices [9]; deploying medical apps on user, group or device bases; and providing access to apps through remote portals [24]. Other mobile device app data security interventions include: ensuring that medical app notifications do not send content to the screen, minimal use of caches, and prohibition of the use of jail-broken devices [9].

**Information technology**

This theme encompasses issues and interventions that are the responsibility of the IT department, in either medical facilities or medical schools. IT issues include: loss of network control [16], employee abuse of guest network [27], lack of secure and efficient hospital communication systems [17], unsecure Wi-Fi [9], bandwidth congestion, lack of mobile access support in the form of intranet access procedures [16], and mobile devices’ lack of compatibility [16,23].

Systems interventions include: developing or soliciting systems for enterprise-wide mobile device management [16,27], point-of-care communication software [16], implementing hospitals’ over-the-air medical mobile app installation [9], providing secure Wi-Fi [27], and improving bandwidth [16]. Other network control interventions include: enterprise standard authentication with the ability to disconnect or block users [9,24], device tracking [22,24], network automated device identification and manual authentication [22], device role-based access control [9,24], keeping network activity logs [24], weekly bandwidth analysis, medical records audit trail [24], and assigning authorized personnel for social media publishing and management [22].
**Education and/or curriculum**

This theme deals with issues and interventions that relate to the state of medical education, specifically the curriculum. Emerging curricular issues include, among others: medical schools’ curricular insufficiency to deal with mobile device use etiquette [17], lack of formal training on assessment of medical app accuracy and risks [25], lack of awareness of patient privacy and confidentiality regulations [18], and lack of mobile device use supervision and feedback [17]. In addition, health professionals’ self-interpretation of reasonable behavior in terms of mobile device use [18] could be linked to issues such of heavy reliance on mobile devices [19], lack of cell phone etiquette [17,18,21], interruptions of patient encounters and educational sessions [17,19,21], distracted doctoring [17,19,21], disregard for patient preferences [17], medical errors [17], poor urgency towards text messages, and distortion of traditional hospital communication [16].

Interventions include: fostering mobile device preferences and mobile device etiquette education to encourage and guide use [23], developing medical school curricula that cover mobile device etiquette [17], educational programs to raise awareness of risks of inappropriate medical app use [25], risk management training and supervision [22], and patient education on and involvement in mobile device use [23].

**Policy**

This theme deals with policy-related issues and interventions that emerge from BYOD-enabled healthcare and medical school environments. Issues of policy in BYOD-enabled environments include: lack of BYOD policy [26], lack of comprehensive IT policy and infrastructure [27], lack of mobile device use policy, and lack of social media policy to control posting of patient confidential information [20].
Interventions for policy issues include the development of: a BYOD policy [16,26], comprehensive IT policy and infrastructure [27], mobile device use policy [16,17,22,23], hospital texting policy [18], comprehensive patient health privacy and confidentiality policies [22], personal devices cleaning and sanitization policies [16], and policies and procedures on employees’ network abuse [27]. Other recommendations include: embedding BYOD policy texts in employment contracts and agreements [9], developing guidelines for privacy and best practices [18], enacting a policy that covers device secondary access to e-mail [22], and establishing BYOD guidelines and procedures [9,23] as well as cell phone etiquette guidelines [19]. It is also recommended that mobile device use boundaries be set to curb their use during surgical procedures, for example [23].

**BYOD guidelines**

This theme deals with the general lessons or recommendations for BYOD enabling or management in the healthcare terrain. Emerging strategic institutional guidelines include: lifting bans and regulating the use of personal mobile devices [19], investing in a BYOD-optimized environment [23], optimizing BYOD monetary savings to mitigate possible risks [16], acquiring BYOD-suitable technologies and system rationalization, and out-sourcing or automating key BYOD administrative tasks [16]. As a guideline, it is vital to understand that a breach in PHI security is a liability for the facility or institution, irrespective of device ownership [16,22], although formal policies could hold individuals accountable [26]. Operational guidelines include: IT environment appraisal [24], improving compliance by collaborating with mobile device users [16], effective use of device in-built capability to control disruption [21], and discouraging mobile device use during patient consultations [23].
DISCUSSION

We explored the literature to identify BYOD policy components (issues, interventions, and guidelines) that could potentially inform BYOD policy development and implementation in healthcare facilities and medical schools. The seven emerging themes were: device management, data security, medical apps, IT, education and/or curriculum, policy, and guidelines.

Challenges and concerns for BYOD in healthcare include inappropriate mobile device use [16,20-23], unsecure mobile device use [9,16,18,21,22], use of unregulated mobile apps [25], unready IT infrastructure [9,16,17], lack of mobile device etiquette [17,18,21], and lack of supporting policies [20,26,27]. Several interventions can be put in place to mitigate these issues. They include authentication controls [16,22-24], regulating unsecure data manipulation [16,18,21-23,27], regulating medical apps [9,24,25], acquiring mobile device management systems [16,27], implementing BYOD or mobile device use policies [16,17,22,23,26,27], and fostering mobile device etiquette [17,23]. Guidelines on BYOD highlight the importance of a decisive enabling of BYOD [19], investment in BYOD technologies [16,23,24], and providing guidance [16,19,22,23].

The results suggest that BYOD remains a complex concept in terms of both its definition and the general understanding thereof [7,10]. BYOD is generally defined as individuals’ ability to use their personal mobile devices in practice and/or learning [7,9,11]. It is therefore ‘the use of personal mobile devices’ that has generally been used to epitomize BYOD [4,7,9,10]. However, the word ‘personal’ as used in the definition of BYOD does not always mean user ownership of mobile devices. It appears to include employees’ or learners’ use of facility-
institutionally owned mobile devices [27], and personally owned devices that are sometimes registered for practice [16,22-24]. As such, it seems that mobile device ownership is not what defines BYOD, but rather that what defines BYOD is ‘mobile device use’ when associated with policy or policies that promote and guide such use [5]. The conceptualization of BYOD as ‘mobile device use’ seems consistent with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations, which place liability of compromised PHI with the healthcare facility, irrespective of device ownership [16,22].

Although the literature suggests that device ownership may not solely be used to conceptualize BYOD, it is nonetheless an important consideration in the development and implementation of BYOD policies. Some interventions such as promoting the use of provisional mobile devices [27], registering personal mobile devices for workplace use [16,22-24], and controlling users’ mobile devices at trade-in or donation [22] seem to suggest that some BYOD-related challenges are possibly linked to mobile device ownership. Such challenges include: difficulties in maintaining control of corporate networks, coping with bandwidth congestion resulting from increased use of personal mobile devices [9,16,22,23], high cases of loss of mobile devices [16,20-23], and use of unsecured mobile devices [16-21]. Therefore, the results seem to suggest that the willingness of healthcare professionals and learners to use personally owned mobile devices for work and learning may not necessarily mean willingness to surrender all control and/or submit to mobile device use policies [16]. It is possible that ‘personal’ remains ‘personal’ in both ownership and use, even if facilities and institutions are responsible for providing and ensuring the safety of BYOD environments.

Two other areas appear to present a challenge in the overall understanding of BYOD. The first challenge is a superficial understanding of BYOD as ‘users bringing their personal
mobile devices for use in the work or learning space’, which can inadvertently result in the misconception that BYOD is a ‘cheap’ initiative [4,7,9,10]. Such understanding could be misleading, because to enable a BYOD environment, one has to have policies that would balance the myriad of challenges with appropriate interventions to optimally achieve BYOD benefits. Beyond a policy, there is a need to invest in appropriate technologies and systems to ensure a safe but accessible BYOD environment [9,16,22,24,27]. Another challenge to the current understanding of BYOD relates to the concept of ‘mobile device’, which seems to suggest an advantage of ‘mobile devices’ over other related computing technologies such as laptops and desktops. Winters [3] suggests that what is actually mobile is the user and not the device. As such, the focus of research and innovation should rather be on what the user does while mobile than on what the device can do.

Despite the complexity in understanding BYOD, the overriding and all-encompassing benefit of and motivation for enabling BYOD in healthcare settings remains ‘convenience’ of access and communication [6]. However, convenience and network security can sometimes seem incompatible [7,10]. For instance, the results suggest a high prevalence of lack of password protection in mobile devices used in healthcare settings [16-21], as medical professionals often feel that password authentication is an inconvenience [9]. This has led to recommendations of ‘convenient authentication’ [9], a possible oxymoron that highlights a potential mismatch of interests between users who need convenience [6] and network and systems administrators who need to implement network controls [16].

The results also suggest policies as potential tools for negotiating the balance between users’ need for convenience [6] and network and systems administrators’ need to implement network controls [16]. There is a broad spectrum of policies that appear in the literature and
relate to various aspects of BYOD. They include: BYOD policy [16,26], mobile device use policy [16,17,22,23], hospital texting policy [18], privacy and confidentiality policy [22], personal devices cleaning and sanitization policy [16], and network abuse policy [27]. In addition, there are also regulatory measures that assist in policy implementation such as device registration [16,22-24]; password protection [18,21]; authentication controls [9,23]; controlled access, downloading, storage and messaging of PHI [16,23]; data transfer appraisal [24]; and controlled medical app environments [9,16,22-25].

The myriad of policies and regulations relating to the implementation of mobile device use can lead to several issues, particularly when there seems to be a pattern of having an intervention (policy or technical) for every issue, possibly making BYOD an aggressive investment [5,6,23,24,26,28,29,40-43]. It is also unclear how, after implementing all the policies and regulations, mobile devices are still able to provide convenience desired by users. The limited literature on the evaluation of BYOD policies also makes it difficult to learn how other healthcare facilities and medical schools have maintained the delicate balance between convenience and security.

Kehoe [27] recommends a single comprehensive BYOD policy that addresses various aspects of mobile device use. However, what seems lacking from the BYOD literature is the approach towards BYOD policy formulation. Ideally, policy formulation should begin with individual, societal and organizational needs analysis [44]. The outcome of such needs analysis should represent a balance between individual and organizational interests [44]. Because IT departments negotiate and implement system controls, they should collaborate with mobile device users in policy formulation to achieve user (employees and learners) buy-in and ultimately a safer BYOD environment [16]. Beyond a consultative approach to BYOD
policy formulation, BYOD policies should address the fluid relationship between healthcare facilities and medical schools. Medical students on clinical rotations, for instance, come in contact with PHI, sometimes with limited awareness of patient privacy and confidentiality regulations [18]. There are also instances of unprofessional mobile device use by medical students and clinicians or medical school lecturers [17-19,21].

In their endeavor to develop BYOD policies, healthcare facilities and medical schools should also attempt and influence mobile device manufacturers [16], medical app developers [15,32], and healthcare professionals [25] through active collaboration to define and shape the future of BYOD. For example, mobile device manufacturers can use healthcare legislation or regulations such as the HIPAA to produce healthcare use-compliant mobile devices [16] and re-consider screen size, touch screen and embedded keypads that are known to contribute to errors in data capturing [16,23,25]. Medical app developers may take into consideration developing regulation-complaint medical apps such as MobiSante, a cell phone-based medical diagnostic tool with an ultrasound probe approved by the US Food and Drug Administration [45]. They can also consider developing medical apps with an offline option to support continuous access to high-quality medical content [25,32], and to also engage clinicians and physicians early in the development of medical apps as opposed to leaving that to the developers, who may lack the necessary medical background [25].

Medical schools can also use policy to promote increased use of technology in the curriculum through provisional mobile devices [27] as at Stanford University’s medical school [46] and the University of Botswana Faculty of Medicine [31-33]. In addition, investments in open-source hardware can allow medical schools and healthcare facilities to study, customize or modify, repair, make, and distribute hardware, thereby reducing reliance on external providers [47]. It is also advisable that in promoting the use of mobile device technologies, a
balance be negotiated between mobile and fixed devices, as fixed devices can be more suitable for some functions such as supporting data collection [48,49]. Mobile devices can be limited by smaller screen sizes [16,23,25,50], variable screen resolutions, more restricted user input and limited processing power [50], all of which can affect user engagement [51].

Ultimately, a comprehensive BYOD policy, even when it is internal, should carefully observe the macro environment and anticipate potential integration of a variety of mobile device uses, especially as healthcare facilities work towards seamless mobile device access and communication [23,32,41,52-56]. That is, the BYOD policy should cater for other mobile device uses such as diagnosis [45,57-61], patient monitoring, follow-up [46,62-66], data collection [43,46,51,67], and medication adherence [68,69]. Integration of mobile devices into hospital systems, especially patient record management [70], including patient participation in computerized patient record management [71], is also worth policy consideration. Other areas of policy consideration include patient self-diagnosis using unregulated medical apps, technology intimidation especially for older physicians, and over-dependency on technology [46].

**STUDY LIMITATIONS**

Although our search was systematic and comprehensive, there is still a possibility that we may have omitted some relevant literature. For example, terms such as ‘mobile gadgets’ may have been ignored despite being instrumental in the search and healthcare. They may be other terms apart from personal digital assistants that may have been overlooked. Despite the inclusion of magazine articles, the review might have omitted other unpublished literature. In addition, a realist review strategy of including conversations with experts and users might have added value to the review [72].
FUTURE RESEARCH
In the light of the paucity in peer-reviewed literature on BYOD implementation, evaluation and policy development in medical schools and healthcare facilities, there is a need for research into the development and effectiveness of BYOD policies and guidelines. This could inform a robust conversation on BYOD implementation in healthcare facilities and medical schools. Such research could also provide answers to questions on what users are willing to do with the device while mobile, and who pays and for what in BYOD [3], particularly if such research considers socio-technical aspects of BYOD implementation and policy development [73].

CONCLUSIONS
The ‘culture’ or ‘habit’ of using personal mobile devices at work and in learning environments is expected to continue growing, due in part to potential benefits for healthcare delivery and medical education. Nonetheless, it is necessary for healthcare facilities and medical schools to develop BYOD policies [16,26,27] rather than an approach of ‘chasing’ issues with interventions. This could ensure that BYOD implementation remains feasible and manageable. Such a comprehensive policy should at least be inclusive of critical elements such as device management, data management, medical app management, IT capacity, and education and curricular readiness and inclusiveness. Even though the immediate cost benefits of implementing BYOD could initially be negative, the long-term cost benefits might prove to be positive as the systems continue to evolve [74,75].

CONTRIBUTORS: MBK, KK, and DK conceived the design of the study and developed the search strategy. KK conducted the search, reviewed titles and abstracts, and developed
and completed the matrix with input from MBK. KK, MBK, and DK analyzed the matrix and identified and agreed on emerging themes. KK developed the draft with input from MBK and DK. All authors contributed to the critical revision of the paper, approved the final draft, and have agreed to be accountable for all aspects of the work.

ACKNOWLEDGEMENTS: The authors would like thank Dr Billy M. Tsimia (BMed, MMed, MSc) for facilitating a workshop on conducting scholarly reviews of literature, from which the conception of the idea of this paper emerged.

FUNDING: This paper is part of a project supported by the Health Resources and Services Administration (HRSA) of the US Department of Health and Human Services (HHS) under grant T84HA22125 (Medical Education Partnership Initiative). The information, content, and conclusions presented in this article are of the authors and should neither be construed as the official position or policy of, nor should any endorsements be inferred by, the HRSA, HHS, or US government.

CONFLICTS OF INTEREST: None

ETHICAL APPROVAL: Not applicable

SUPPLEMENTARY MATERIAL: Matrix (Appendix A)
REFERENCES


9. Al Ayubi SU, Pelletier A, Sunthara G, Gujral N, Mittal V, Bourgeois FC. A mobile app development guideline for hospital settings: maximizing the use of and minimizing the
security risks of “bring your own devices” policies. JMIR mHealth uHealth 2016;4(2):e50. PMID:27169345


27. Zahadat N, Blessner P, Blackburn T, Olson BA. BYOD security engineering: a


44. Huang CC, Lee PY, Chen PY, Liu TY. Design and implementation of a smartphone-based portable ultrasound pulsed-wave doppler device for blood flow measurement. IEEE Trans Ultrason Ferroelectr Freq Control 2012;59(1):182-188. PMID:22293750
46. Vincent CJ, Niezen G, O’Kane AA, Stawarz K. Can standards and regulations keep up with health technology? JMIR mHealth uHealth 2015;3(2):e64. PMID:26041730
52. Walsh SH. The clinician’s perspective on electronic health records and how they can affect patient care. BMJ 2004;328(7449):1184-1187. PMID:15142929


70. Jones R, Rogers R, Roberts J, Callaghan L, Lindsey L, Campbell J, Thorogood M,


