International Journal of Medical Informatics 119 (2018) 94–102

Contents lists available at ScienceDirect

International Journal of Medical Informatics

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

Review article

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

Khutsafalo Kadimo[a,*], Masego B. Kebaetse[b], Dineo Ketshogileng[a], Lovie Edwin Seru[c], Kagiso B. Sebina[d], Carrie Kovarik[e], Kutlo Balotlegi[b]

[a] Department of Library Services, University of Botswana, Private Bag UB 0022, Gaborone, Botswana
[b] Department of Medical Education, University of Botswana, Gaborone, Botswana, Private Bag UB 0022, Gaborone, Botswana
[c] Communication and Study Skills Unit, University of Botswana, Private Bag UB 0022, Gaborone, Botswana
[d] Botswana-University of Maryland School of Medicine Health Initiative, P. O. Box 203258 Bontleng, Gaborone, Botswana
[e] Department of Dermatology, Dermatopathology, and Infectious Diseases, University of Pennsylvania, 2 Maloney Building, 3600 Spruce Street, Philadelphia, PA, USA

ARTICLE INFO

Keywords:
Bring-your-own-device (BYOD)
mobile devices
Mhealth
Mlearning
Medical education
Healthcare facilities

ABSTRACT

Background: Enabling personal mobile device use through a bring-your-own device (BYOD) policy can potentially save significant costs for medical schools and healthcare facilities, as they would not always have to acquire facility-owned devices. The BYOD policy is also perceived as a driver for balancing user needs for convenience with institutional needs for security. However, there seems to be a paucity in the literature on BYOD policy development, policy evaluation, and evaluation of mobile device implementation projects.

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

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: Several themes emerging from the analysis 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 while the policy theme seems to be the comprehensive solution that synergizes BYOD implementation.

Conclusion: Rather than an approach of 'chasing' issues with interventions, 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 medical schools and healthcare facilities.

1. Introduction

Bring-your-own-device (BYOD) is generally conceptualized as employees' use of personal mobile devices to complete work related tasks [1–13]. Driven by rapid advances in information communication technologies (ICT) and recent increase in use of consumer ICTs in the workplace, BYOD is considered as a form of IT consumerization [14,15]. IT consumerization refers to the use of market originating tools (both devices and software) in the workplace [15,16]. As a form of market perspective IT consumerization, BYOD refers to the use of institutionally sanctioned, and personally owned consumer tools in the workplace [15]. The notion of institutional approval in BYOD is in contrast to another form of IT consumerization known as shadow information technologies (shadow IT). Sometimes referred to as shadow systems, shadow IT focuses on the use of market originating third party cloud-based software services and tools without organizational approval such as saving institutional data on personal cloud-based systems. [14,15,17–20].

* Corresponding author at: Department of Library Services, University of Botswana, 4775 Notwane Rd., Private Bag UB 0022, Gaborone, Botswana.
E-mail address: khutsafalo.kadimo@mopipi.ub.bw (K. Kadimo).

https://doi.org/10.1016/j.ijmedinf.2018.09.013
Received 1 June 2018; Received in revised form 30 July 2018; Accepted 12 September 2018
1386-5056/ © 2018 Elsevier B.V. All rights reserved.

With users in some cases possessing individual systems that are sometimes better than enterprise systems [15], the use of consumer IT in the workplace occurs with or without a BYOD strategy [21]. Mobile device use in itself does not constitute BYOD unless there is an associated policy (a plan for achieving set goals) [22]. The use of consumer IT and third-party cloud-based software is considered a 'defiant' habit in that it often betrays organizational IT standards, rules, directives, procedures, and routines [14,15,17–20]. BYOD therefore, describes the 'implemented environments' that are enabled by formal policies or BYOD programs [8,11,15] to leverage the benefits of mobile device use while fostering a safe and appropriate mobile device use environment [12]. Concerted effort is required to establish and implement policies that balance the integration of both information and communication technologies (ICTs), and information use factors to guide the implementation of BYOD [22].

Several benefits can be realized by enabling mobile device use through a BYOD policy. Medical schools and healthcare facilities can save significant costs, as they would not have to acquire facility-owned devices [5,7,10,12,23]. Additionally, employees would potentially be more efficient [7,10,12,23], and innovative [14,15,24,25] when working with their personally chosen technology or mobile devices, harnessing their experiences of using such technology [7,10,12,14,15,23–25]. This could improve productivity [7,10,12,14,15,23–25], job satisfaction [14,15,24,25] and customer satisfaction [7,10,12,23] through the enhancement of communication and patient care [7,10,12,23,26]. Personal mobile device use can provide for convenient access, retrieval, storage, and sharing of information [9,27,28] in preferred formats [1], and sometimes without the internet by both students and employees [29]. Also, the use of mobile devices can lead to increased patient satisfaction and increased access to care takers [30].

The use of mobile devices in the workplace without a guiding BYOD strategy or policy [4,31,32], mobile device use policies [12,23] and regulations [33] remains a challenge for medical schools and healthcare facilities. Such unguided mobile device use can precipitate challenges such as unsecure [32,34–38] and inappropriate use of mobile devices [10,12,34,36,38,39], and medical applications (apps) [23]. These challenges are in most cases attributable to lack of network controls [10,23], education [7,33,35,36] and technologies and systems for managing communication [34,40,41]. Medical schools and healthcare facilities need adequate guidance to leverage benefits of mobile device use [4,31,32,34,40,42,43] while protecting patient privacy and confidentiality [32,39,40,43–45] and managing issues of data security and quality [4,32,33,41,43,44,46–49]. In healthcare facilities compromised patient health information (PHI) due to inappropriate mobile device use can come with high costs [9,48] and serious consequences that would harm the image of the facility [33]. Consequently, the enactment of guiding policies is seen as a critical measure for ensuring effective BYOD implementation [34,40,42,43].

In spite of the potential utility of BYOD policy or guiding strategy, there seems to be a paucity in the medical education and healthcare facility literature on BYOD policy development, policy evaluation, and evaluation of mobile device implementation projects [6,50] to inform efficient BYOD implementation. Such a paucity in literature can potentially contribute to the lack of guidance in developing, implementing, studying, and evaluating BYOD policies in medical schools and healthcare facilities. Nonetheless, available literature seems to highlight possible components of BYOD policies that could 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 can possibly inform BYOD policy development and implementation in medical schools and healthcare facilities.

2. Methods

2.1. Study background

In 2013 the University of Botswana Faculty of Medicine launched the mLearning project in which academic staff, specialists trainees, and students in the clinical phase of the undergraduate phase of the program were provided institutional devices preloaded with mobile data, learning and point-of-care resources [51–53]. Since the project was funded through a grant, we decided to explore BYOD as way to expand and sustain our project beyond the life of the grant. We anticipated that beyond the grant, continuing to provide institutional devices and mobile data would no longer be feasible. As such, the assumption was that BYOD implementation would transfer the costs of procuring devices and mobile data to end-users. Also, the responsibility for technical support would shift to end-users. Nonetheless, end-users would leverage institutional network infrastructure and professional support of librarians and information technology specialists to maximize the use of their devices for learning, teaching, research and patient care. In light of the intimate relationship between the medical school and the training healthcare facility, we had serious concerns about how the devices might be used without conscious regard for patient privacy and confidentiality. As a result, we pursued the development of an institutional policy and enabling set of guidelines, as well as user support instructions for our BYOD implementation.

Our initial plan was to review the literature on BYOD policies in order to glean ideas that could inform our own BYOD policy formulation. However, the implementation of BYOD in medical schools is complicated by the fluid and complementary use of mobile devices in medical schools and healthcare facilities. That is, the same device used for learning and or teaching (mlearning) is also used for healthcare delivery (mhealth) [51,52,54]. As such, while this co-existence of mlearning and mhealth leverages potential benefits of mobile device use, it complicates BYOD policy formulation in that such policy needs to address both mlearning and mhealth. Therefore, our review had to address literature form both medical schools and healthcare facilities.

The preliminary search seemed to suggest 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.

2.2. Methodological overview

We conducted a scoping 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 [55–58]. To further ensure methodological rigor, we paid attention to the principles of systematic literature review such as having a clear purpose for the review, having more than one person in appraise articles, having a clear inclusion/exclusion criteria (purposive sampling), and considering alternative perspectives [55,57]. We reviewed the literature broadly, identifying what was already known, gaps in knowledge, and what still needed to be considered [58], and sought to derive a 'conceptual contribution' from the literature [56]. This review, therefore, is intended to expand on current understanding of BYOD implementation [57].

2.3. Data searching and 'mining'

A search and 'mining' of the literature was conducted between July and August 2016. We developed a search strategy using the following basic keywords and their synonyms: mobile devices, cell phones, bring-

Download English Version:

https://daneshyari.com/en/article/11032469

Download Persian Version:

https://daneshyari.com/article/11032469

Daneshyari.com