Healthier Lives, Digitally Enabled
M. Merolli et al. (Eds.)

doi:10.3233/SHTI210002

Bring-Your-Own-Device Usage Trends in Australian Hospitals – A National Survey

Tafheem Ahmad WANI [a,1], Antonette MENDOZA [a] and Kathleen GRAY [b]
[a] *School of Computing and Information Systems, The University of Melbourne*
[b] *Centre for Digital Transformation of Health, The University of Melbourne*

Abstract. Background: Healthcare is among the leading industries which drives the use of personal devices for work purposes (BYOD). However, allowing BYOD for healthcare workers comes at a cost, as it puts sensitive information assets such as patient data residing on personal devices at risk of potential data breaches. Objective: Previous review of the literature has highlighted the dearth of empirical studies in hospital settings regarding BYOD usage. As such, this paper aims to report BYOD usage trends in Australian hospitals through a national survey, first of its kind in Australia. Methods: An anonymous survey was conducted online among health IT personnel, asking them about their experiences about BYOD usage in their hospitals. 28 responses were collected based on public Australian hospitals, which included 21 hospital groups and 7 standalone hospitals, likely to represent more than 100 hospitals in total. Survey responses were quantitatively analysed through descriptive statistical analysis and cross tabulation. Results: BYOD is allowed in majority of the hospitals, and among all major staff groups, with doctors being the leading group. Participants ranked reasons for allowing BYOD, and most of them were related to improvement in clinical productivity, efficiency and mobility for clinical staff. Challenges were generally related to data security such as patient data breaches and compliance with data security laws, according to them. More than two thirds of hospitals had a cybersecurity officer employed, and CIOs were the most dominant group who held responsibility for managing BYOD within the hospital. Conclusion: This paper provides a starting point for better understanding of BYOD usage in a complex healthcare environment based on empirical evidence, one which highlights the security-usability conundrum, confirming previous literature themes.

Keywords. BYOD, bring-your-own-device, cybersecurity, health, hospital, privacy

1. Introduction

'Bring-your-own-device' or BYOD is a common practice in workplaces, where employees use their personal mobile devices such as smartphones, tablets, laptops for carrying out professional or work-related tasks [1]. Healthcare is one of the leading industries driving BYOD usage [2]. Healthcare professionals typically perform a range of work-related tasks using their personal devices: accessing electronic medical records, clinical documentation, photography, diagnostic or drug information results, and for communication or collaboration with fellow staff or patients [3, 4] . Not only does BYOD improve the productivity and efficiency of clinicians, it also enhances their mobility and allows them to provide patient care within and outside hospital or clinic workplaces [5]. For example, the COVID-19 pandemic has created an upsurge in use of BYOD by hospital staff for purposes such as telehealth consultations and remote work [6, 7].

[1] Corresponding Author, Tafheem Ahmad Wani, School of Computing and Information Systems, The University of Melbourne, Parkville, Victoria, Australia 3010, E-mail: twani@student.unimelb.edu.au.

However, BYOD is a major challenge for hospitals due to data security concerns and is seen as one of the biggest healthcare IT challenges [8]. Healthcare sees the greatest number of data breaches of all industries, not only in Australia but world-wide, with BYOD being a major reason [9, 10, 11]. Hospitals typically don't have any control on the number and type of devices their employees use, nor their device usage behaviour, which increases the risk of data breaches, including patient data. Each device added to the hospital network is a potential cybersecurity threat [12]. Also, hospital compliance with patient data privacy laws is difficult in a BYOD environment [9, 13]. Continuing the COVID-19 example, the increase in remote work among healthcare workers during the pandemic has led to several data breaches where BYOD was a major cause [6, 7, 14].

Previous reviews of both academic and grey literature identified social, technical and managerial issues associated with BYOD usage [12, 15]. However, they showed that there is a dearth of empirical studies of BYOD usage in healthcare settings, especially in Australia, given its unique health IT context as well as a different set of laws concerning healthcare data breaches [12, 16, 17]. Hence, this paper reports on actual BYOD usage trends in Australian hospitals. Information about access obtained via BYOD, socio-technical security measures, benefits and further analysis was also asked as part of this survey, but this would be covered in a future publication due to this paper's size limits.

2. Methodology

A national Australian survey recruited volunteers among health IT personnel with an overview knowledge of BYOD usage within their respective hospitals. The survey asked questions about participants' experiences with BYOD practices in mid-to large size hospitals, with human research ethics approval (Ethics ID: 1955486.1) obtained from the University of Melbourne. Preliminary research based on literature review and a conceptual framework developed by the authors was used to frame survey questions [12, 15, 18]. The survey was setup online using the Qualtrics survey platform. Only anonymous data was collected, with no information requested which could individually identify a participant or a hospital. This was done to make sure that sensitivities about potentially pinpointing a specific organisation's practices or gaps are carefully recognised. The survey used Qualtrics IP filtering to avoid duplication of responses.

The survey was promoted through webinars and social media groups (particularly associated with cyber security) of professional organisations such as Australian Institute of Digital Health (AIDH), Health Information and Management Systems Society (HIMSS) and platforms such as LinkedIn. It was also sent to all state government health CIOs or people in similar positions for information and circulation. Responses were collected during a four-month period from March to June 2020. An anonymous link was used for distribution, which was carefully circulated to avoid duplication.

28 responses were collected from participants based in public hospitals from four Australian states. 21 survey responses were based on BYOD practices in hospital groups, while 7 concerned standalone hospitals. Given that each hospital group comprises an average of 3-7 hospitals in Australia, the number of hospitals reflected in the survey is likely more than 100 – compared to a total of 693 public hospitals in Australia [19]. Survey questions were analysed quantitatively through descriptive statistical analysis and cross tabulation, using Qualtrics analysis platform, as well as Excel. The results presented here provide an initial picture of BYOD usage in Australian hospitals.

3. Results

3.1. Individual and Hospital Characteristics

The survey was completed by IT personnel with different designations including Chief Information Officer (CIO), Chief Information Security Officer (CISO), IT Director, IT Manager, IT Infrastructure Manager, and Information Security Manager. 11 participants (39.29%) had worked in the hospital or hospital group about which they supplied information for up to 5 years, 9 participants (32.14%) for 6-10 years, and 8 participants (28.57%) for more than 10 years.

The hospitals about which information was supplied, were diverse. With respect to their principal location which participants described, 8 responses (28.57%) were based on hospitals or hospital groups in inner city locations, 8 responses (28.57%) were suburban hospital or hospital group based, 8 responses (28.57%) based on regional centre hospitals or hospital groups and 4 responses (14.29%) based on hospital groups having both a metropolitan and regional presence. With respect to staff size, most surveys reflected large hospital settings. 24 responses (85.71%) were based on hospitals or hospital groups with staff over 1000, 3 responses (10.71%) with 500-1000 staff size and 1 response (3.57%) based on a hospital organisation with staff size less than 500.

3.2. BYOD Usage Trends

3.2.1. BYOD Usage Permission

22 participants (78.57%) said that BYOD was allowed in their hospital/hospital group. Only 5 participants (17.86%) said that BYOD wasn't allowed. One participant (3.57%) said that the policy regarding allowing use of BYOD was not clearly specified to the staff. Out of the 5 participants who said BYOD wasn't allowed in their hospital/hospital group, 4 participants (80%) were unsure if it will be allowed in the next 2 years, whereas 1 participant (20%) said that it won't be allowed even after that. No-one was certain that BYOD would be allowed in the next 2 years. Cross tabulation analysis further reveals that BYOD is allowed in majority of metropolitan hospitals and in hospitals with a large staff size, as opposed to regional hospitals. Specific details on exact distribution across different types of hospitals can be found in Table 1.

Table 1. Cross tabulation analysis on BYOD usage permission based on location and staff size

Hospital Type	Total Count	Whether BYOD Allowed or Not		
Principal Location		**Yes**	**No**	**Not Sure**
Inner City	8	8 (100%)	0 (0%)	0 (0%)
Suburban	8	8 (100%)	0 (0%)	0 (0%)
Regional Centre	8	3 (37.5%)	4 (50%)	1 (12.5%)
Other	4	3 (75%)	1 (25%)	0 (0%)
Staff Size				
Less than 500	1	1 (100%)	0 (0%)	0 (0%)
Between 500 - 1000	3	2 (66.67%)	1 (33.33%)	0 (0%)
More than 1000	24	19 (79.17%)	4 (16.67%)	1 (4.16%)
GRAND TOTAL	**28**	**22 (78.57%)**	**5 (17.86%)**	**1 (3.57%)**

3.2.2. BYOD Usage by Staff

Clinical, IT and administrative staff were allowed to use BYOD among the hospital/hospital groups which allowed it. Out of 23 hospitals / groups which allowed BYOD, 21 (91.30%) allowed BYOD for doctors and 20 (86.96%) allowed it for IT staff. This was followed by administrative and clerical staff - 17 (73.91%), nurses - 16 (69.57%), diagnostic and allied health professionals - 16 (69.57%) and domestic and other personal care staff - 11 (47.83%).

3.2.3. Reasons for Allowing and Disallowing BYOD

Participants were asked to rank reasons for allowing BYOD in hospitals/hospital groups, based on a number of options given in the survey. According to majority of the participants, improvement in clinical productivity or efficiency among staff was the topmost reason for allowing BYOD in their hospital, with 14 participants (60.87%) out of 23 ranking it number 1. Based on average ranking score, this was followed by: improvement in employee satisfaction (ranked 2), making teleworking easier (ranked 3), saving money (ranked 4), difficulty in enforcing bans on BYOD use (ranked 5) and reducing device procurement workload on IT (ranked 6).

Among hospitals/hospital groups not allowing BYOD, 3 participants (60%) out of 5 selected patient data breaches as the topmost reason for not allowing BYOD. Lesser reasons included IT management/administration overhead (ranked 2), compliance with healthcare data privacy laws (ranked 3), security management costs (ranked 4), reimbursement for staff (ranked 5), inadvertent mixing of private and professional data (ranked 6) and regulating user behaviour (ranked 7).

3.2.4. Major Challenges Related to BYOD

For hospitals or hospital groups allowing BYOD, participants were asked to rank challenges related to BYOD, based on a number of options given in the survey. The top ranked challenge was compliance with healthcare data privacy laws, with 10 participants (43.48%) out of 23 ranking this as number 1. This was followed by patient data breaches (ranked 2), regulating user behaviour (ranked 3), security management costs (ranked 4), IT management/administration overhead (ranked 5), reimbursement for staff (ranked 6) and inadvertent mixing of private and professional data (ranked 7).

3.2.5. BYOD Program Ownership

Program ownership refers to allocating the overall responsibility of a particular program to a unit or person for better accountability. 21 participants (95.45%) out of 22 whose organisations allowed BYOD said that their hospitals had allocated the overall responsibility for the program to a staff role. 19 participants (90.47%) said that the CIO held ownership of the BYOD program, 1 participant (4.76%) said that the CTO was the owner and 1 participant (4.76%) said that the CEO was responsible for the program.

3.2.6. Cybersecurity Personnel Employed in the Hospital/Hospital Group

19 participants (67.86%) said that their hospital/hospital group had a dedicated cybersecurity officer for managing information security affairs. Further distribution is provided in Table 2 using cross-tabulation analysis.

Table 2. Cross tabulation analysis of whether cybersecurity personnel employed or not.

Hospital Characteristic	Total Count	Whether Cybersecurity Personnel Employed	
Principal Location		**Yes**	**No**
Inner City	8	6 (75%)	2 (25%)
Suburban	8	6 (75%)	2 (25%)
Regional Centre	8	5 (62.5%)	3 (37.5%)
Other	4	2 (50%)	2 (50%)
Staff Size			
Less than 500	1	1 (100%)	0 (0%)
Between 500 - 1000	3	1 (33.33%)	2 (66.67%)
More than 1000	24	17 (70.83%)	7 (29.17%)
GRAND TOTAL	**28**	**19 (67.86%)**	**9 (32.14%)**

4. Discussion

The hospital industry in Australia follows the global trend, as survey responses suggest that BYOD is allowed by majority of the hospitals and across all staff groups. The survey findings also indicate that the familiarity and convenience of using personal devices for work by clinicians is thought to boost their clinical productivity and save their time. Out of the different clinician groups, BYOD usage was reported to be particularly high among doctors; this may be due to the nature of a doctor's work across multiple hospitals and other clinical settings. On the other hand, nurses may be more strongly affiliated with a single hospital, and BYOD usage may be constrained by more interaction with in-hospital record-keeping systems, or greater infection control considerations. Further research is under way involving clinical participants, to shed more light on whether a differential approach may be required for different clinical roles, when choosing whether to allow BYOD and/or what services to allow.

The survey suggests that the topmost issues associated with BYOD use relate to security, which includes patient data breaches and non-compliance with data privacy laws, confirming themes from the literature. The same reason was quoted by participants for not allowing BYOD. The data also implies that regional hospitals may also face the additional challenge of lack of budget to maintain cybersecurity requirements. This is a huge concern for hospitals as BYOD is a major contributor for health data breaches. It is also becoming difficult for hospitals to comply with strict government regulations as highlighted previously. This might be the reason that it was ranked as the number 1 challenge concerning BYOD use.

This indicates the need for security and usability balance, as the authors have highlighted previously [12, 15]. To address this challenge, hospitals not only need to leverage their existing IT security technologies, but also to have BYOD policies and training programs for staff which can provide them guidance for productive, flexible and safe use of BYOD to ensure proper compliance. Hospitals where ownership of BYOD programs is the responsibility of the CIO, or of a dedicated cybersecurity officer, indicate steps in the right direction.

This survey is first of its kind to be reported in Australia. Its major limitation is that there may be a degree of imprecision associated with data collection, as it was very important to elicit anonymous responses from senior hospital insiders, without compromising reputations or further jeopardising privacy of these organisations. Features such as automatic IP filtering and survey protection was used to avoid this. Also, the diversity of the nature of hospital settings represented in this survey also makes it

unlikely or minimal. Further, it does not reflect practices in the private hospital sector, or in primary and community healthcare organisations. This paper presents only the first part of a larger study by the authors exploring the people, policy and technology factors in balancing the risks and benefits of BYOD in hospitals. Further research will provide a deeper analysis of the technical, social and managerial aspects of BYOD security.

Overall, this work contributes a new understanding of BYOD in Australian hospitals. It raises the profile of this ubiquitous and pragmatic aspect of health information technology, and therefore provides the start of a roadmap for improving careful and responsible BYOD use.

References

[1] D. Arregui, S. Maynard, and A. Ahmad, "Mitigating BYOD information security risks," 2015. Available: http://minerva-access.unimelb.edu.au/handle/11343/56627.
[2] "BYOD (Bring Your Own Device) Market Analysis, Market Size, Application Analysis, Regional Outlook, Competitive Strategies and Forecasts, 2016 To 2024," Hexa Research, Dec. 2016.
[3] A. Nerminathan, A. Harrison, M. Phelps, S. Alexander, and K. M. Scott, "Doctors' use of mobile devices in the clinical setting: a mixed methods study," *Intern. Med. J.*, vol. 47, no. 3, pp. 291–298, 2017, doi: 10.1111/imj.13349.
[4] M. Moreau and G. Paré, "Early clinical management of severe burn patients using telemedicine: a pilot study protocol," *Pilot Feasibility Stud.*, vol. 6, no. 1, p. 93, Jul. 2020, doi: 10.1186/s40814-020-00637-7.
[5] J. Williams, "Left to Their Own Devices How Healthcare Organizations Are Tackling the BYOD Trend,"
[6] *Biomed. Instrum. Technol.*, vol. 48, no. 5, p. 327, Sep. 2014.
[7] Bitglass, "Bitglass 2020 BYOD Report: Remote Work Drives BYOD, but Security Not Keeping Pace," 2020. https://www.bitglass.com/press-releases/bitglass-2020-byod-report-remote-work-drives-byod-but-security-not-keeping-pace
[8] J. Davis, "Must-Have Telehealth, Remote Work Privacy and Security for COVID-19," *HealthITSecurity*, Mar. 31, 2020.
[9] J. L. Schiff, "The 4 biggest healthcare IT headaches," *CIO*, May 23, 2017. https://www.cio.com/article/3197698/healthcare/the-4-biggest-healthcare-it-headaches.html
[10] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/j.maturitas.2018.04.008.
[11] J. Davis, "Health Sector Most Targeted by Hackers, Breach Costs Rise to $17.76B," *HealthITSecurity*, Jun. 09, 2020.
[12] OAIC, "Notifiable Data Breaches scheme 12-month insights report," 2019. [Online]. Available: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/.
[13] T. A. Wani, A. Mendoza, and K. Gray, "Hospital Bring-Your-Own-Device Security Challenges and Solutions: Systematic Review of Gray Literature," *JMIR MHealth UHealth*, vol. 8, no. 6, p. e18175, 2020, doi: 10.2196/18175.
[14] E. Snell, "4 Key Concerns in Healthcare Mobile Security Options," *HealthITSecurity*, Aug. 17, 2017.
[15] J. Davis, "Remote Attacks on Cloud Service Targets Rose 630% Amid COVID-19," HealthITSecurity, Jun. 2020. Available: https://healthitsecurity.com/news/remote-attacks-on-cloud-service-targets-rose-630-amid-covid-19.
[16] T. A. Wani, A. Mendoza, and K. Gray, "BYOD in Hospitals-Security Issues and Mitigation Strategies," in *Proceedings of the Australasian Computer Science Week Multiconference*, New York, NY, USA, 2019, p. 25:1–25:10, doi: 10.1145/3290688.3290729.
[17] J. E. Moyer, "Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage."
[18] *J. Hosp. Librariansh.*, vol. 13, no. 3, pp. 197–208, Jul. 2013, doi: 10.1080/15323269.2013.798768.
[19] N. Zahadat, P. Blessner, T. Blackburn, and B. A. Olson, "BYOD security engineering: A framework and its analysis," *Comput. Secur.*, vol. 55, pp. 81–99, Nov. 2015, doi: 10.1016/j.cose.2015.06.011.
[20] S. Schlarman, "The People, Policy, Technology (PPT) Model: Core Elements of the Security Process,"
[21] *Inf. Syst. Secur.*, vol. 10, no. 5, pp. 1–6, 2006, doi: 10.1201/1086/43315.10.5.20011101/31719.6.
[22] AIHW, "Hospital resources 2017–18: Australian hospital statistics, At a glance," AIHW, 2019. [Online]. Available: https://www.aihw.gov.au/reports/hospitals/hospital-resources-2017-18-ahs/contents/at-a-glance.