Journal of Universal Computer Science, vol. 24, no. 5 (2018), 634-645
submitted: 23/1/18, accepted: 28/4/18, appeared: 28/5/18 © J.UCS

Relating Mobile Device Use and Adherence to Information Security Policy with Data Breach Consequences in Hospitals

Simon Vrhovec
(University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia
simon.vrhovec@fvv.uni-mb.si)

Blaž Markelj
(University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia
blaz.markelj@fvv.uni-mb.si)

Abstract: Critical infrastructure is a high value target in the real world and cyberspace. A failure to protect the critical infrastructure in the cyberspace could lead to serious financial and material losses and violate the effective functioning of a country. In this paper, we will focus on healthcare as an important part of the critical infrastructure. An important part of the healthcare infrastructure are hospitals. Hospital personnel is increasingly using mobile devices in their everyday work to improve patient care. Hospitals may however fail to adequately address the use of mobile devices and adapt their information security policies in time. Hospital personnel may use both their personal and work mobile devices for everyday work. Sometimes they do it without adhering to an adequate hospital information security policy. The objective of this paper is to study the relation between the use of mobile devices, adhering to hospital information security policy and perceived consequences of data breaches. An exploratory survey (N = 95) has been conducted in a Slovenian hospital. Respondents were asked about the use of their personal and work mobile devices for accessing medical data, adhering to the hospital information security policy, and the perceived consequences of data breaches for themselves, the hospital and the patients. The results show that perceived personal consequences are negatively correlated with personal and work mobile device use for work. Also, adhering to information security policy is positively correlated with perceived data breach consequences for both the patients and the hospital.

Keywords: Hospital, Mobile devices, Information security, Data breach, Health care
Categories: H.4.3, J.3, K.6.5, L.7

1 Introduction

Critical infrastructure is defined as a system whose malfunction or destruction would have a serious negative impact on health and safety of people, could lead to serious financial and material losses and would violate the effective functioning of a country [Petrov, Stoianov and Tagarev 2018]. Main types of critical infrastructure encompass agriculture and food industry, banking and finance, chemical industry, government facilities, communications, power plants, dams, water system, energy system, national defense and domestic security, transport system, emergency services and healthcare [Petrov et al. 2018]. Critical infrastructure is considered a high value target and its cybersecurity is an integral part of any serious security system [Caire 2018, Korobiichuk, Hryshchuk, Mamarev, Okhrimchuk and Kachniarz 2018]. Cyber-operations against critical infrastructure may be undertaken to deny the use of the infrastructure to its operator or to exploit the its services to improve its own capabilities [Caire 2018].

Critical infrastructure systems encompass facilities, services, rules, personnel, documents, management methodology and procedures of processing and exchanging information [Petrov et al. 2018]. Protecting such complex systems from technical and human perspectives may be challenging and poorly researched especially regarding the latter perspective. There is a need for skilled, competent, knowledgeable and motivated personnel in the area of critical infrastructure cybersecurity [Howard and Arimatéia da Cruz 2017, Oliver and Haney 2017]. Additionally, this personnel may use mobile devices to access critical infrastructure resources, services and applications which complicates protecting the critical infrastructure even further [Jannati and Bahrak 2017].

In this paper, we focus on the use of mobile devices in hospitals which represent a part of the healthcare critical infrastructure. Mobile devices are introduced into everyday work of hospital personnel to improve work processes and patient care [Al Ayubi et al. 2016, Motulsky et al. 2016, Sharpe and Hemsley 2016]. Mobile devices are omnipresent in general as well as in healthcare. Hospital personnel are able to use both their work and personal mobile devices for everyday work even though the information security policy of hospitals may not allow it [Sharpe and Hemsley 2016, Vrhovec 2016, Whipple, Allgood and Larue 2012]. Bring-your-own-device (BYOD), i.e., using personal mobile devices at work, may be preferred by hospitals relatively often as it enables a significant lowering of the costs needed to provide all personnel with work mobile devices which are then used only in the hospital [Al Ayubi et al. 2016, Ehrler, Blondon, Baillon-Bigotte and Lovis 2017, Faulds et al. 2016, Motulsky et al. 2016].

New issues accompany the adoption of work and personal mobile devices by the hospital personnel and in recent years incidents related to mobile devices accounted for most data breaches in health care [Bitglass 2014]. Hospitals are thus required to adapt the hospital information security policies to include and adequately address the use of both work and personal mobile devices and to promote and enforce them among hospital personnel [Al Ayubi et al. 2016, Faulds et al. 2016, Motulsky et al. 2016]. Ensuring that the hospital personnel adheres to the hospital information security policy may however prove to be quite challenging [Giles-Smith, Spencer, Shaw, Porter and Lobchuk 2017, Sher, Talley, Cheng and Kuo 2017, Vrhovec 2016].

The objective of this paper is to study the relation between the use of mobile devices for accessing medical data, adhering to hospital information security policy and perceived consequences of potential data breaches. To achieve this, we conducted an explorative survey in a Slovenian hospital. Respondents were asked about the use of their personal and work mobile devices for accessing medical data, adhering to the hospital information security policy, and the perceived consequences of data breaches for themselves, the hospital and the patients.

The paper is structured as follows. First, we present the theoretical background on the use of mobile devices in hospitals and how the hospital personnel perceive data breach consequences, and develop the hypotheses. Next, we present the research methodology. Results are presented in chapter four and discussion follows in chapter five. We conclude the paper with some concluding remarks and directions for further work.

2 Theoretical Background

2.1 Mobile devices in hospitals

Mobile device use in hospital settings offers a variety of new possibilities [Sharpe and Hemsley 2016]. Hospital personnel may use them as an alternative to workstations for accessing medical data which enables them to access it from wherever needed, the patient room, a meeting, the patient's home or elsewhere [HIMSS Analytics 2014, Storbrauck 2015]. Use of mobile devices tends to increase work satisfaction of the hospital personnel and improves direct communication between them and the patients [HIMSS Analytics 2014, The Office of the National Coordinator for Health Information Technology 2015]. Although studies show multiple benefits of mobile device use, some drawbacks have also been pointed out, e.g., frequent interruptions may distract the hospital personnel which can result in medical errors [Ross and Forgie 2012, Tran et al. 2014, Westbrook 2010].

Mobile devices may be costly for hospitals to introduce and maintain [Al Ayubi et al. 2016]. Hospitals first need to invest into both software and hardware which both notably increase the complexity of the hospitals' technological ecosystem. This commonly includes introducing new or upgraded wireless network infrastructures that may also be used by external parties, such as patients and their visitors therefore introducing new potential attack vectors. Network segmentation is commonly used to separate internal and external parties in the wireless network infrastructure to tackle these issues. To lower the costs, hospitals may encourage the use of personal mobile devices at work [Al Ayubi et al. 2016, Martínez-Pérez, de la Torre-Díez and López-Coronado 2015]. BYOD is also convenient for the hospital personnel as they are already familiar with the device making it a win-win situation [Vrhovec 2016]. Not everything is good about BYOD though. Accessing medical data from a device that is used for both personal and work use is a security issue per se. This is a fundamental trade-off between data security and data access [Bai, Jiang and Flasher 2017]. The hospital has few means to control the cybersecurity of the mobile device, e.g., by checking for VPN connection or disabling access for rooted or jailbroken devices [Al Ayubi et al. 2016]. There is also the potential for unprofessional behavior due to using personal mobile devices [Robinson et al. 2013, Wu et al. 2013]. Additionally, there are privacy concerns regarding the use of unsecure communication channels, such as non-encrypted e-mail, for communicating patient health information between patients and the hospital personnel [Wu et al. 2013].

The hospital information security policy needs to be adapted to the de facto use of mobile devices in the hospital. Research shows that over 90 percent of the hospital personnel use their own mobile devices at work to access medical data [Bitglass 2014, Martínez-Pérez et al. 2015]. However, only 38 percent of hospitals define a formal policy of mobile device use [Martínez-Pérez et al. 2015, Storbrauck 2015, The Office of the National Coordinator for Health Information Technology 2015]. Low awareness of cybersecurity threats and hospital information security policies of the hospital personnel seem to be a major challenge [Vrhovec 2016]. Despite attempts to ensure information security and patient privacy, most of recent data breaches seem to be related to mobile devices [Bitglass 2014].

2.2 Data breach consequences

Hospital personnel may perceive the consequences of a data breach on three levels. A data breach may directly affect the patients whose data has been exposed. Medical data can be used to acquire direct financial gain, commit an electronic fraud, steal the medical identity, or extort the victims [Storbrauck 2015]. Medical identity theft is wide-spread and can have severe financial and medical consequences if a patient's medical record is contaminated with medical data of a third person [Bitglass 2014, McDavid 2013]. Therefore, we develop the first set of hypotheses:

H1a. Perceived consequences of a data breach for the patients are negatively correlated with work mobile device use.

H1b. Perceived consequences of a data breach for the patients are negatively correlated with personal mobile device use.

H1c. Perceived consequences of a data breach for the patients are positively correlated with adhering to the hospital information security policy.

The data breach may have an impact on the hospital where the data breach has occurred. The patients trust hospitals that they visit with their most sensitive and private information and hospitals aim to keep their reputation as trustworthy organizations by adequately protecting patients' medical data [Bitglass 2014]. Hospitals try to avoid data breaches as recovering the lost reputation due to a data breach is a tough job [Bitglass 2014]. In addition to losing reputation and patients, hospitals could face high fines and lawsuits from patients [Bitglass 2014]. These arguments suggest the second set of hypotheses:

H2a. Perceived consequences of a data breach for the hospital are negatively correlated with work mobile device use.

H2b. Perceived consequences of a data breach for the hospital are negatively correlated with personal mobile device use.

H2c. Perceived consequences of a data breach for the hospital are positively correlated with adhering to the hospital information security policy.

The data breach may also affect the person directly responsible for it, i.e., the hospital employee using the mobile device at the time of the data breach. Depending on the hospital policy, a data breach may significantly affect a hospital employee's career or there may even be no consequences for the hospital employee at all. We developed the following set of hypotheses based on the above:

H3a. Perceived personal consequences of a data breach are negatively correlated with work mobile device use.

H3b. Perceived personal consequences of a data breach are negatively correlated with personal mobile device use.

H3c. Perceived personal consequences of a data breach are positively correlated with adhering to the hospital information security policy.

3 Methods

To test our model, we conducted an exploratory survey in a Slovenian hospital. The hospital did not have a formal information security policy neither on work nor on personal mobile devices. Even though personal mobile devices were commonly used for everyday work and work mobile devices were being introduced, the hospital failed to update its information security policy accordingly.

The survey was conducted among the hospital personnel participating in information security training organized by a third-party cybersecurity company. The training was mandatory however absence was not penalized. The participants had several opportunities to attend the training due to their unpredictable work commitments. Randomly chosen groups of attendants were asked to complete the survey before attending the training. In total, 150 surveys have been administered and 95 respondents returned the survey representing a response rate of 63 percent. The number of missing values ranged from 1.1 to 3.2 percent except for work device use which had 7 missing cases (7.4 percent). The distribution of the respondents' roles suggests that physicians were underrepresented in the sample which may be attributed to their generally low interest in attending any training. The shares of nurses and administration personnel matches exactly their shares in the hospital indicating their appropriate representation.

All constructs were measured by using single-items as a very high degree of parsimony was required [Bunderson and Boumgarden 2010, Lee, Delene, Bunda and Kim 2000]. Under specific conditions, the predictive validity of single-item measures is comparable to the predictive validity of multi-item measures [Bergkvist and Rossiter 2007, Diamantopoulos, Sarstedt, Fuchs, Wilczynski and Kaiser 2012, Lee et al. 2000]. Due to the exploratory nature of the study, the use of single-item measures thus seems reasonable. The survey items are presented in the Appendix A.

Characteristic	**N**	**Percent**
Health care professional		
Physician	2	2.11
Nurse	77	81.05
Administration personnel	9	9.47
Not specified	7	7.37
Gender		
Male	16	16.84
Female	77	81.05
Not specified	2	2.11

Table 1: Demographic characteristics

Table 1 presents the respondents' demographics.

4 Results

Table 2 includes means (M) and standard deviations (SD) for all studied constructs.

Code	**Construct**	**M**	**SD**
DBCP	Perceived data breach consequences for patients	6.56	0.811
DBCH	Perceived data breach consequences for hospital	6.45	0.863
PCDB	Perceived personal consequences of a data breach	6.65	0.617
WMDU	Work mobile device use	2.77	1.849
PMDU	Personal mobile device use	1.60	1.177
AISP	Adhering to information security policy	5.62	1.146

Table 2: Descriptive statistics

Some constructs did not follow a normal distribution therefore we calculated Kendall's Tau non-parametric rank correlation coefficients between them. Table 3 presents the correlation matrix. The results show support for hypotheses H2c and H3b ($p < 0.01$) and hypotheses H1c and H3a ($p < 0.05$). Other results are however nonsignificant and do not support any of the remaining hypotheses H1a, H1b, H2a, H2b and H3c.

Construct	**DBCP**	**DBCH**	**PCDB**	**WMDU**	**PMDU**	**AISP**
DBCP		0.475^{***}	0.364^{***}	-0.166	-0.103	0.219^{*}
DBCH	**0.475^{***}**		0.257^{**}	-0.106	-0.142	0.249^{**}
PCDB	**0.364^{***}**	**0.257^{**}**		-0.197^{*}	-0.268^{**}	0.041
WMDU	-0.166	-0.106	**-0.197^{*}**		0.321^{**}	-0.128
PMDU	-0.103	-0.142	**-0.268^{**}**	**0.321^{**}**		-0.080
AISP	**0.219^{*}**	**0.249^{**}**	0.041	-0.128	-0.080	

Table 3: Correlation matrix

The results of testing the hypotheses are presented in Figure 1. Other interesting results in addition to the test of our hypotheses are also included in Figure 1. First, there are significant positive correlations between perceived personal consequences of a data breach and perceived data breach consequences for hospital and patients ($p < 0.001$). Next, the correlation between perceived data breach consequences for hospital and patients is also significant and positive ($p < 0.01$). Finally, there is a significant positive correlation between work and personal mobile device use ($p < 0.01$).

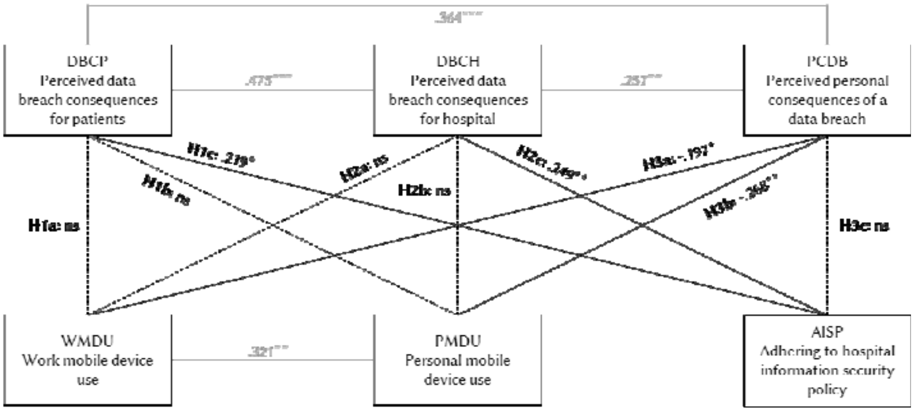
.364***
DBCP
Perceived data breach consequences for patients
.475***
DBCH
Perceived data breach consequences for hospital
.251**
PCDB
Perceived personal consequences of a data breach
H1c: .219*
H2a: ns
H2c: .249**
H3a: -.197*
H1b: ns
H2b: ns
H3b: -.268**
H1a: ns
H3c: ns
WMDU
Work mobile device use
.321**
PMDU
Personal mobile device use
AISP
Adhering to hospital information security policy

Figure 1: Hypotheses testing results

5 Discussion

The results of this explorative study show support for only 4 out of the 9 developed hypotheses. The confirmation of hypotheses H1c and H2c shows the importance of perceived data breach consequences for the hospital and the patients in adhering to the hospital information security policy. The higher the perceived data breach consequences for the hospital and the patients the higher the adherence to the hospital information security policy. It is however surprising that hypothesis H3c has not been confirmed as it suggests that the perceived personal consequences of a data breach do not play an important role in adhering to the hospital information security policy. This suggests that the hospital personnel do not take the hospital information security policy for their own despite the relatively high scores of this construct (5.62 ± 1.146). In other words, these findings suggest that the hospital personnel do not identify completely with the hospital regarding its information security policy. Nevertheless, the hospital personnel respect the need to protect the hospital and the patients from data breaches by adhering to the hospital information security policy.

The confirmation of hypotheses H3a and H3b and non-confirmation of the remaining hypotheses H1a, H1b, H2a and H2b suggests quite the opposite for mobile device use. Higher perceived personal consequences of a data breach seem to hinder the adoption of mobile devices. This may be attributed to the lack of a clear hospital information security policy on mobile devices as the hospital had no policy for personal mobile devices and work mobile devices were only being formally introduced. Perceived data breach consequences for the hospital or the patients however do not seem to play an important role in the use of mobile devices by the hospital personnel. This is quite surprising as it suggests that the hospital personnel do not consider the consequences that the use of their mobile device may have for either the hospital or the patients. The difference seems to vary depending on the type of mobile device. Work mobile device use is more loosely correlated with perceived personal consequences of a data breach than personal mobile device use. Also, nonsignificant correlations related to work mobile device use seem to be closer to the significant one than the nonsignificant correlations related to personal mobile device use. This gives us a hint that the hospital personnel could only loosely relate the use of their personal mobile devices to data breach consequences for hospitals and patients. Again, this could still be attributed to the lack of a clear hospital information security policy on mobile devices.

There are strong correlations between all three perceived data breach consequences. These results suggest that the hospital personnel relate their personal consequences more to the consequences for the patients than those for the hospital. This shows that the hospital personnel first think of their patients and only after of their employer. In a way, this supports the finding that they do not identify well with the hospital regarding its information security policy.

The use of work and personal mobile devices is relatively low (2.77 ± 1.849 and 1.60 ± 1.177, respectively) which can be attributed to the fact that the mobile devices are just being introduced. There is a strong correlation between work and personal mobile device use. This suggests that the hospital personnel could use personal mobile devices for work only after they have started using the work mobile devices. Another explanation would be that they are even able to use personal mobile devices for work after the hospital information system adds the mobile device access functionality and they become aware of it. This highlights the importance of covering both work and personal mobile device use in the hospital information security policy.

5.1 Limitations and further work

As with all research, the reader should consider the limitations of this study when interpreting its results. First, the survey was done in a single subject organization. The studied hospital could be considered as a typical hospital in the process of introducing mobile devices to its processes. Nevertheless, the reader should be cautious when generalizing the findings of this study. Further research should aim to include more hospitals from different cultural contexts and different stages of mobile device adoption. Second, the use of single-item measures in the survey has its drawbacks as it does not allow reliability and validity analysis of the survey instrument. Further research should aim to use multi-item measures which allow rigorous testing of the survey instrument. Third, the respondents may not have had the same notion of the information security policy and a data breach entail as they were not provided any explanation prior to the survey. It may thus be possible that the responses were not indicative of the same concept. Further research should consider focusing on clear and real scenarios when preparing new items. Fourth, the subjects of the study were all health care professionals. A study comparing different health care professionals (e.g., administration personnel, physicians and nurses) would provide useful insights into the differences between them. Fifth, it would be also useful to incorporate level of experience in the healthcare domain as a control variable in the analysis. Sixth, experiments may be conducted to determine the effect of different kinds of information security training (e.g., lectures, practical examples, e-learning etc.). These experiments should include surveys before and after (in 30 and 180 days) the training to determine the short- and middle-term effect of different kinds of information security training.

6 Conclusion

This paper aims at providing better understanding of how to ensure information security in healthcare which is an important part of the critical infrastructure. The presented explorative study reports on the use of mobile devices in hospitals and perceived data breach consequences. The study hints at the challenges that information security professionals face when introducing mobile devices and the respective information security policies in hospital settings. The main findings show that the hospital personnel consider data breach consequences for the hospital and the patients when adhering to the hospital information security policy. They however do not relate data breach consequences for themselves to adhering to the hospital information security policy suggesting they do not see personal benefits in it. Hospitals are therefore faced with the need to improve this issue by either better promoting its information security policy among the hospital personnel or updating it in a way that the hospital personnel would see some benefits in it.

When using mobile devices, the hospital personnel seem to consider only the consequences of data breaches for themselves. No correlation to the data breach consequences for the hospital or the patients suggests that they have difficulties relating the use of their work or personal mobile devices to consequences of data breaches or perhaps data breaches in general. Hospitals may strive to raise the awareness of hospital personnel about the relation of mobile devices to data breaches and their potential impact on the patients and the hospital as a whole. The hospital personnel need to understand that if the data is breached in any way, including due to the use of their personal or work mobile device, it can affect both the hospital and the patients in addition to themselves. At the same time, the hospital personnel need to understand the risks of using both personal and work mobile devices as well as the protective measures, such as regularly locking the mobile device and using encryption, to tackle them.

References

[Al Ayubi et al. 2016] Al Ayubi, S. U., Pelletier, A., Sunthara, G., Gujral, N., Mittal, V., Bourgeois, F. C.: ‘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 and uHealth, Vol. 4, No. 2 (2016), p. e50. https://doi.org/10.2196/mhealth.4424

[Bai, Jiang and Flasher 2017] Bai, G., Jiang, J. (Xuefeng), Flasher, R.: ‘Hospital Risk of Data Breaches’; JAMA Internal Medicine, Vol. 177, No. 6 (2017), p. 878. https://doi.org/10.1001/jamainternmed.2017.0336

[Bergkvist and Rossiter 2007] Bergkvist, L., Rossiter, J. R.: ‘The Predictive Validity of Multiple-Item Versus Single-Item Measures of the Same Constructs’; Journal of Marketing Research, Vol. 44, No. 2 (2007), pp. 175–184. https://doi.org/10.1509/jmkr.44.2.175

[Bitglass 2014] Bitglass: ‘The 2014 Bitglass Healthcare Breach Report’; (2014). Retrieved from http://pages.bitglass.com/rs/bitglass/images/WP-Healthcare-Report-2014.pdf

[Bunderson and Boumgarden 2010] Bunderson, J. S., Boumgarden, P.: ‘Structure and Learning in Self-Managed Teams: Why “Bureaucratic” Teams Can Be Better Learners’; Organization Science, Vol. 21, No. 3 (2010), pp. 609–624. https://doi.org/10.1287/orsc.1090.0483

[Caire 2018] Caire, J.: ‘Human factors in cybersecurity for transportation systems’; In WIT Transactions on the Built Environment (Vol. 176) (2018), pp. 405–414. https://doi.org/10.2495/UT170351

[Diamantopoulos, Sarstedt, Fuchs, Wilczynski and Kaiser 2012] Diamantopoulos, A., Sarstedt, M., Fuchs, C., Wilczynski, P., Kaiser, S.: ‘Guidelines for choosing between multi-item and single-item scales for construct measurement: a predictive validity perspective’; Journal of the Academy of Marketing Science, Vol. 40, No. 3 (2012), pp. 434–449. https://doi.org/10.1007/s11747-011-0300-3

[Ehrler, Blondon, Baillon-Bigotte and Lovis 2017] Ehrler, F., Blondon, K., Baillon-Bigotte, D., Lovis, C.: ‘Smartphones to Access to Patient Data in Hospital Settings: Authentication Solutions for Shared Devices’; In 14th International Conference on Wearable Micro and Nano Technologies for Personalized Health, pHealth 2017. Eindhoven, The Netherlands: IOS Press (2017), pp. 73–78. https://doi.org/10.3233/978-1-61499-761-0-73

[Faulds et al. 2016] Faulds, M. C., Bauchmuller, K., Miller, D., Rosser, J. H., Shuker, K., Wrench, I., et al.: ‘The feasibility of using “bring your own device” (BYOD) technology for electronic data capture in multicentre medical audit and research’; Anaesthesia, Vol. 71, No. 1 (2016), pp. 58–66. https://doi.org/10.1111/anae.13268

[Giles-Smith, Spencer, Shaw, Porter and Lobchuk 2017] Giles-Smith, L., Spencer, A., Shaw, C., Porter, C., Lobchuk, M.: ‘A Study of the Impact of an Educational Intervention on Nurse Attitudes and Behaviours toward Mobile Device Use in Hospital Settings’; Journal of the Canadian Health Libraries Association / Journal de l’Association Des Bibliothèques de La Santé Du Canada, Vol. 38, No. 1 (2017), pp. 0–2. https://doi.org/10.5596/c17-003

[HIMSS Analytics 2014] HIMSS Analytics: ‘2014 Mobile Devices Study’; (2014). Retrieved from http://www.himssanalytics.org/research/essentials-brief-mobile-devices-study

[Howard and Arimatéia da Cruz 2017] Howard, T. D., Arimatéia da Cruz, J. de: ‘Stay the course: Why trump must build on obama’s cybersecurity policy’; Information Security Journal: A Global Perspective, Vol. 26, No. 6 (2017), pp. 276–286. https://doi.org/10.1080/19393555.2017.1385115

[Jannati and Bahrak 2017] Jannati, H., Bahrak, B.: ‘An improved authentication protocol for distributed mobile cloud computing services’; International Journal of Critical Infrastructure Protection, Vol. 19 (2017), pp. 59–67. https://doi.org/10.1016/j.ijcip.2017.10.003

[Korobiichuk, Hryshchuk, Mamarev, Okhrimchuk and Kachniarz 2018] Korobiichuk, I., Hryshchuk, R., Mamarev, V., Okhrimchuk, V., Kachniarz, M.: ‘Cyberattack Classificator Verification’; In Advances in Intelligent Systems and Computing (Vol. 635) (2018), pp. 402–411. https://doi.org/10.1007/978-3-319-64474-5_34

[Lee, Delene, Bunda and Kim 2000] Lee, H., Delene, L. M., Bunda, M. A., Kim, C.: ‘Methods of Measuring Health-Care Service Quality’; Journal of Business Research, Vol. 48, No. 3 (2000), pp. 233–246. https://doi.org/10.1016/S0148-2963(98)00089-7

[Martínez-Pérez, de la Torre-Díez and López-Coronado 2015] Martínez-Pérez, B., de la Torre-Díez, I., López-Coronado, M.: ‘Privacy and Security in Mobile Health Apps: A Review and Recommendations’; Journal of Medical Systems, Vol. 39, No. 1 (2015), p. 181: 1-8. https://doi.org/10.1007/s10916-014-0181-3

[McDavid 2013] McDavid, J. P.: ‘HIPAA Risk Is Contagious: Practical Tips to Prevent Breach’; The Journal of Medical Practice Management, Vol. 29, No. 1 (2013), pp. 53–55.

[Motulsky et al. 2016] Motulsky, A., Wong, J., Cordeau, J.-P., Pomalaza, J., Barkun, J., Tamblyn, R.: 'Using mobile devices for inpatient rounding and handoffs: an innovative application developed and rapidly adopted by clinicians in a pediatric hospital'; Journal of the American Medical Informatics Association, Vol. 10, No. 2 (2016), p. ocw107. https://doi.org/10.1093/jamia/ocw107

[Oliver and Haney 2017] Oliver, D., Haney, M.: 'Preparing the next cyber-resilient workforce through cross-pollination education'; In 2017 Resilience Week (RWS). IEEE (2017), pp. 44–49. https://doi.org/10.1109/RWEEK.2017.8088646

[Petrov, Stoianov and Tagarev 2018] Petrov, L., Stoianov, N., Tagarev, T.: 'Critical Information Infrastructure Protection Model and Methodology, Based on National and NATO Study'; In Advances in Intelligent Systems and Computing (Vol. 582) (2018), pp. 350–357. https://doi.org/10.1007/978-3-319-59415-6_34

[Robinson et al. 2013] Robinson, T., Cronin, T., Ibrahim, H., Jinks, M., Molitor, T., Newman, J., Shapiro, J.: 'Smartphone Use and Acceptability Among Clinical Medical Students: A Questionnaire-Based Study'; Journal of Medical Systems, Vol. 37, No. 3 (2013), p. 9936. https://doi.org/10.1007/s10916-013-9936-5

[Ross and Forgie 2012] Ross, S., Forgie, S.: 'Distracted doctoring: Smartphones before patients?'; Canadian Medical Association Journal, Vol. 184, No. 12 (2012), pp. 1440–1440. https://doi.org/10.1503/cmaj.120462

[Sharpe and Hemsley 2016] Sharpe, B., Hemsley, B.: 'Improving nurse-patient communication with patients with communication impairments: Hospital nurses' views on the feasibility of using mobile communication technologies'; Applied Nursing Research, Vol. 30 (2016), pp. 228–236. https://doi.org/10.1016/j.apnr.2015.11.012

[Sher, Talley, Cheng and Kuo 2017] Sher, M.-L., Talley, P. C., Cheng, T.-J., Kuo, K.-M.: 'How can hospitals better protect the privacy of electronic medical records? Perspectives from staff members of health information management departments'; Health Information Management Journal, Vol. 46, No. 2 (2017), pp. 87–95. https://doi.org/10.1177/1833358316671264

[Storbrauck 2015] Storbrauck, L.: 'Mobile Device Use: Increasing Privacy and Security Awareness for Nurse Practitioners'; La Salle University (2015).

[The Office of the National Coordinator for Health Information Technology 2015] The Office of the National Coordinator for Health Information Technology: 'Guide to Privacy and Security of Electronic Health Information'; (2015), p. 62.

[Tran et al. 2014] Tran, K., Morra, D., Lo, V., Quan, S. D., Abrams, H., Wu, R. C.: 'Medical students and personal smartphones in the clinical environment: The impact on confidentiality of personal health information and professionalism'; Journal of Medical Internet Research, Vol. 16, No. 5 (2014), p. e132. https://doi.org/10.2196/jmir.3138

[Vrhovec 2016] Vrhovec, S. L. R.: 'Challenges of mobile device use in healthcare'; In P. Biljanović (Ed.), 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2016). Opatija, Croatia: Croatian Society for Information and Communication Technology, Electronics and Microelectronics (2016). https://doi.org/10.1109/MIPRO.2016.7522357

[Westbrook 2010] Westbrook, J. I.: 'Association of Interruptions With an Increased Risk and Severity of Medication Administration Errors'; Archives of Internal Medicine, Vol. 170, No. 8 (2010), p. 683. https://doi.org/10.1001/archinternmed.2010.65

[Whipple, Allgood and Larue 2012] Whipple, E. C., Allgood, K. L., Larue, E. M.: 'Third-year medical students' knowledge of privacy and security issues concerning mobile devices'; Medical Teacher, Vol. 34, No. 8 (2012), pp. e532–e548. https://doi.org/10.3109/0142159X.2012.670319

[Wu et al. 2013] Wu, R. C., Lo, V., Morra, D., Wong, B. M., Sargeant, R., Locke, K., et al.: 'The intended and unintended consequences of communication systems on general internal medicine inpatient care delivery: a prospective observational case study of five teaching hospitals'; Journal of the American Medical Informatics Association, Vol. 20, No. 4 (2013), pp. 766–777. https://doi.org/10.1136/amiajnl-2012-001160

Appendix A

All items were scored on a seven-point Likert scale from 1 (I strongly disagree) to 7 (I strongly agree).

Construct	Items
Perceived data breach consequences for patients	Data breaches are very harmful for the affected patients.
Perceived data breach consequences for hospital	Data breaches are very harmful for the hospital.
Perceived personal consequences of a data breach	Data breaches are very harmful for the one responsible.
Work mobile device use	I use my work mobile device to access patient data very often.
Personal mobile device use	I use my personal mobile device to access patient data very often.
Adhering to information security policy	I always adhere to the hospital information security policy.