Check for updates

Practice and Innovation Article

HIMJ

Health Information Management Journal
1–7
© The Author(s) 2019
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1833358319851684
journals.sagepub.com/home/himj
SAGE

Wearable devices in healthcare: Privacy and information security issues

Liezel Cilliers

Abstract

Background: Mobile health has provided new and exciting ways for patients to partake in their healthcare. Wearable devices are designed to collect the user's health data, which can be analysed to provide information about the user's health status. However, little research has been conducted that addresses privacy and information security issues of these devices. **Objective:** To investigate the privacy and information security issues to which users are exposed when using wearable health devices. **Method:** The study used a cross-sectional survey approach to collect data from a convenience sample of 106 respondents. **Results:** Half of the respondents did not understand the need to protect health information. There also appeared to be a general lack of awareness among respondents about the information security issues surrounding their data collected by wearable devices. **Conclusion:** Users were not knowledgeable about the privacy risks that their data are exposed to or how these data are protected once collected. **Implications:** Users of wearable devices that collect personal information about health need to be educated about privacy and information security issues to which they are exposed when using these devices.

Keywords (MeSH)

wearable electronic devices; wearable devices; wearable technology; information security; information protection; cyber security; patient data privacy; privacy; confidentiality; integrity; availability; health information management

Introduction

Technology, such as wearable devices, can be used to encourage individuals to be more active and make good lifestyle choices. Wearable devices collect vast amounts of data from users making use of different behavioural and physiological sensors, which monitor their health status and activity levels (Ogundele et al., 2018). However, the collection of personal data in unprecedented volumes does raise privacy and security concerns for the user (Martínez-Pérez et al., 2015; Ogundele et al., 2018). Potential harmful consequences of privacy breaches could include discriminatory profiling, manipulative marketing and data breaches (Montgomery et al., 2018).

This article reviews the literature relevant to the privacy and information security issues of wearable devices and presents findings of an original study that examined privacy and information security issues associated with the use of wearable health devices.

Literature review

The number of overweight, obese or morbidly obese adults in South Africa was estimated to be 65% in 2012 (Shisana et al., 2013), while Malambo et al. (2016) reported that 49% of adults were physically inactive. A sedentary lifestyle is ranked ninth among risk factors for mortality in the country.

Wearable devices interface with smartphones and personal computer software to collect a wide variety of data (Farnell and Barkley, 2017). Wearable devices include dedicated health monitors, fitness bands and smartwatches. These devices are commercially available and becoming more popular in healthcare. A quarter of Americans have a smartwatch or fitness tracker with worldwide sales of these devices predicted to be close to 110 million units in 2018 (DuFour et al., 2017; Huckvale et al., 2015). The benefits of the devices include to improve fitness and nutrition, lose weight, reduce stress, break bad habits through haptic feedback (vibration) and provide general information to the individual about their health (DuFour et al., 2017; Montgomery et al., 2018; Ogundele et al., 2018). All of these functions enable individuals to participate in, and take accountability for, their healthcare (Ngamntwini and Cilliers, 2018; Statista, 2016).

University of Fort Hare, South Africa

Accepted for publication April 30, 2019.

Corresponding author:
Associate Professor Liezel Cilliers, University of Fore Hare, 50 Church Street, East London 5201, South Africa.
E-mail: lcilliers@ufh.ac.za

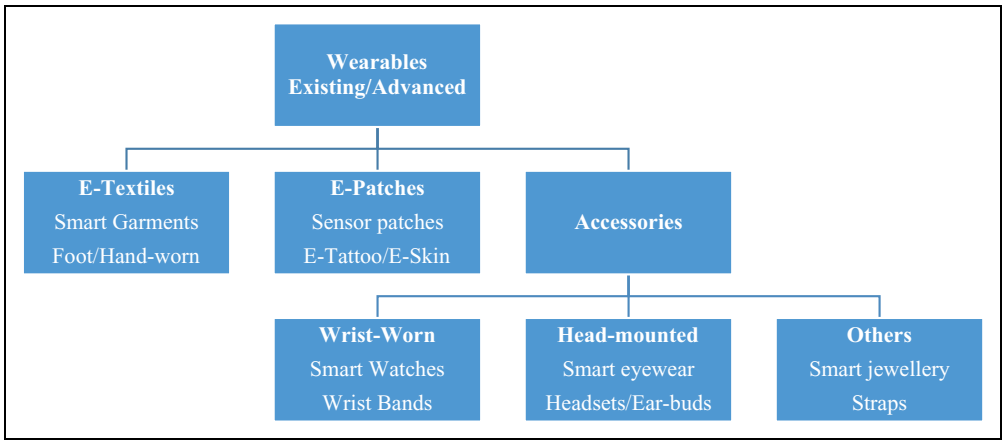

Figure 1. Categories of wearable devices (Seneviratne et al., 2017).

M-health and wearables

Wearable devices are considered a support aid for health services as they provide patients with the ability to monitor their vital signs and identify harmful trends early that could support the diagnoses of chronic diseases (Seneviratne et al., 2017). Healthy behaviour is encouraged by tracking activity levels and providing feedback to enable goal setting which can be shared with interested stakeholders such as healthcare providers (Adibi, 2014). Seneviratne et al. (2017) proposed a framework to identify the various wearable devices that are available for health purposes as indicated in Figure 1. Wrist-worn devices include smartwatches with a touchscreen display, while wristbands are mainly used for fitness tracking but do not have a touchscreen display.

Wearable devices must collect data to be useful. There are two types of data collection that are possible for healthcare. Wearable devices can collect data either automatically through use of the sensors or by the user manually entering data into the device (Wolf et al., 2016). Examples of data that can be collected include location – GPS; quality of surrounding air – sensor attached to the phone; food consumed – logged manually; activity/movements and sleep patterns – accelerometers, pedometer and altimeters; muscle function and coordination – pressure sensors; skin conductance as a proxy for arousal – sensor attached to the phone; temperature and fertile periods – thermometer and electrodermographs; heart rate, blood pressure and blood oxygen – heart rate sensors, electrocardiograms, oximeters and digital camera/flash; psychological disorders and personality traits – social media use; involvements with friends; behavioural patterns and activities when using the smartphone; and measuring cognitive functions and brain activity – brain wearable and cognitive sensors. (Genuth, 2015; Piwek et al., 2016; Scholz, 2012; Tana et al., 2017; Wolf et al., 2016) Collected data are transferred wirelessly to a mobile application or database where these data can be analysed using statistics and presented with visualisation techniques that show the changes over time (Zhou et al., 2015). This information can then be shared via the Internet with healthcare providers to make informed decisions about the user's healthcare (Meingast et al., 2006).

Privacy and wearables

Health information is regarded as the most confidential of all types of personal information (Mehraeen et al., 2016). Privacy is defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967: 2). Montgomery et al. (2018) have stated that in the future, data collected from multiple sources, such as wearable devices and electronic health records, will be combined to provide a complete overview of the health status of the individual. Many users are concerned that they will not have control over what data are collected, when the data will be collected and how the data will be used (Katurura and Cilliers, 2017). More disconcerting is the issue of ownership of the data that is collected from the user. Currently, the data are not owned by the user but rather by the company that produces the wearable device. The user only has access to the aggregated summary of their data, while the raw data can be sold to third parties (Piwek et al., 2016). These issues raise serious privacy concerns for the individual making use of wearable devices (Katurura and Cilliers, 2017).

There are many security threats that users are exposed to when making use of wearable devices. Typically, data that are collected through a wearable device are stored by the company in one database, which has the potential to expose all users if there is a privacy breach (Els and Cilliers, 2017). Recently, the Pentagon acknowledged that the fitness-tracking app Strava© revealed the location of US soldiers in war-torn areas of Syria and Iraq. The "heatmap" feature of the Strava fitness-tracking app was able to reveal the location of US military facilities in Syria and other conflict zones as well as some troop movements. It was further reported that Strava allowed users de-anonymised user-share data to reveal a recorded user's name, speed and even heart rate (Drape, 2018).

Security threats can typically be divided into external threats such as hackers, viruses and worms and internal threats such as accidental loss of the data (Allard et al., 2010). Measures to protect users' data rest on three fundamental pillars of information security: the confidentiality,

integrity and availability triad (Fernández-Alemán et al., 2013). *Confidentiality* refers to the "'process that ensures that information is accessible only to those authorised to have access to it" (Fernández-Alemán et al., 2013: 542). Anonymising the data, where the features that can identify individuals are removed, is often not sufficient to protect the privacy of the user as algorithms can cross-reference wearable-generated biometric data with other "digital traces" of users' behaviour to predict personality traits and risk-taking behaviours (de Montjoye et al., 2013; Lambiotte and Kosinski, 2015). *Data integrity* is concerned with the measurement and quality of the data that are collected (Fernández-Alemán et al., 2013: 542). Experiments have shown that measurements of different wearable devices may differ by as much as 25% (Blobel et al., 2016; Piwek et al., 2016). *Availability of the data* refers to the "property of being accessible and usable upon demand by an authorised entity" (Fernández-Alemán et al., 2013: 543). This presents a difficulty when a healthcare worker may need the data from a patient's wearable device to assist with patient care but is unable to access it because they are not authorised to do so. Additionally, the data must be anonymised to protect the privacy of the patient (Meingast et al., 2006).

There are three vulnerable security areas related to the collection of health data from a wearable device. These threats are associated with: the individual making use of the wearable device to collect data, (physical interference and capacity); data in transit between the device and software program; and storage of the aggregated data in a database (Els and Cilliers, 2017).

Physical interference and capacity

The human factor is often recognised as the weakest link in security; therefore, situational perception and risk awareness play a leading role in the adoption and implementation of security mechanisms (Bellekens et al., 2016). Common threats that occur in this area are that the user can misplace, lose or have the wearable device (e.g. a smartphone) stolen, which enables an unauthorised individual to access confidential information stored on the device (Els and Cilliers, 2017). While owners are responsible for protecting their own privacy on their device, several studies have found that users lack the technical knowledge to implement security measures on their smartphones or wearable devices (Cilliers et al., 2018; Park and Drevin, 2016). Also, smartphones and wearable devices have a smaller screen size in comparison to desktop computers, which makes navigation and reading difficult. Many users do not want to read the privacy policy when they install health applications on their smartphone as the font is too small (Ngamntwini and Cilliers, 2018). Therefore, they may not be aware of the security measures that are necessary to safeguard their health information. The limited storage capacity of these devices also means that the security software on the device may not be sufficient (Els and Cilliers, 2017).

Data in transit

Smartphones have been used for sensitive transactions such as online banking or shopping in recent years, which means that the number of malware that targets these devices have also increased proportionally (Park and Drevin, 2016). When data are in transit, they may be susceptible to eavesdropping, such as sniffing (the process of monitoring and capturing all the packets passing through a given network) or tapping (hardware device used to access the data flowing across a computer network), message alteration or traffic analysis attacks (Els and Cilliers, 2017). Eavesdropping is the unauthorised real-time interception of private communication, and these attacks are significant security threats to wearable systems as they can expose a user's personal information to an attacker (Seneviratne et al., 2017).

As data transmission between wearable devices typically makes use of wireless or Bluetooth technologies, the data are prone to be modified or altered. In these types of attacks, the data are modified as hackers can change the content of exchanging packets or change the timestamp of data packets (Seneviratne et al., 2017). Traffic analysis attacks are the process of monitoring traffic exchanged between wearables and smartphone or a software programme from which inferences from patterns of the communication can be made to track users, detect their activities or identify the user (Das et al., 2016). Hackers, which have become the leading cause of breaches concerning health data, may attempt to use the data to steal a user's identity (Filkins et al., 2016). Once data are stored and analysed in a software programme, these data may be vulnerable to malware, such as viruses or worms, hackers or file-sharing tools (Els and Cilliers, 2017). Additionally, information may be disclosed inadvertently by an individual with access to the information, allowing disclosure beyond intended purposes, such as financial fraud or to humiliate the user (Els and Cilliers, 2017; Filkins et al., 2016).

Data in storage

User do not know how their personal information is secured in the database by the company that owns their data. The user trusts that their personal information is securely stored and that the developers of the mobile application comply with privacy and security regulations (Els and Cilliers, 2017). The problem is compounded as the device is manufactured and sold in different countries, which may have different privacy legislation. Privacy accreditation programs, where mobile applications are subject to formal assessment or peer review, is a recent development and remains largely untested in the context of wearable devices (Wright, 2014). The best recourse that the user can hope for is that the mobile application marketplace and regulators will intervene to safeguard their best interests (Huckvale et al., 2015).

Preventative security measures, or "hard trust" mechanisms, are put in place from a technical point of view (Varadharajan, 2009). Hard trust mechanisms include

Table 1. Demographics and wearable device information from the study population.

Gender	Male	Female			
	32 (30.19%)	74 (69.18%)			
Age (years)	<20	21–30	31–40	41–50	<50
	4 (3.77%)	65 (61.32%)	22 (20.75%)	10 (9.43%)	5 (4.72%)
Why did you buy the mobile health device?	Fitness	Entertainment	Status	Part of a package deal/gift	Other
	67 (63.21%)	9 (8.49%)	2 (1.89%)	16 (15.09%)	12 (11.32%)
How long have you had the device?	Less than 6 months	6–12 months	More than 12 months		
	48 (45.28%)	33 (31.13%)	25 (23.58%)		
What type of mobile health device do you have?	Mobile application	Apple watch	Fitbit	Other	
	31 (29.25%)	24 (22.64%)	40 (37.74%)	11 (10.37%)	

Table 2. Privacy concerns.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I am familiar with my mobile health device's Information Security Policies and how they protects my information/privacy	12 (11.32%)	18 (16.98%)	21 (19.81%)	29 (27.36%)	26 (24.53%)
I understand that health information is considered "sensitive" or "confidential"	24 (22.64%)	31 (29.25%)	21 (19.81%)	21 (19.81%)	9 (8.49%)
I am familiar with how my mobile health device transmits, stores, label and handle my sensitive information	12 (11.32%)	13 (12.26%)	25 (23.58%)	36 (33.96%)	20 (18.87%)

authenticity controls, encryption, algorithms and audits, which are fairly static (Pearson, 2012). In contrast, "soft trust" relies on human emotion, perception and past experiences with the wearable device and social influence. Attributes of the wearable device such as reliability, dependability and perceived competence will all determine how secure the citizens perceive the device to be (Suna et al., 2011; Varadharajan, 2009).

The literature suggests there are various information security threats that could cause privacy breaches from wearable devices. This study examined the privacy and information security issues associated with wearable health devices.

Method

This study employed a quantitative survey approach, with a convenience sampling method used to recruit study participants. Data were analysed using descriptive statistics in SPSS V25. The questionnaire used in this study as the data collection tool was based on the certified information security manager curriculum of the Information Systems Audit and Control Association, which is an independent, nonprofit, global association that engages in the development, adoption and use of globally accepted information system, knowledge and practices. The instrument used consisted of two sections and 23 items overall. Section A (5 items) solicited demographic information from respondents, while Section B (18 items) measured the privacy and information security concerns of the respondents on a five-point Likert-type scale (1 = *strongly disagree* to 5 = *strongly agree*). Empirical reliability for the questionnaire was tested using Cronbach's α.

A pilot study was conducted to pretest the questionnaire among a sample of 10 respondents who were not included in the subsequent main study. Suggestions and amendments from this process were used to refine the research instrument for the main study. The pilot study provided for the face and content validity of the questionnaire.

Data were collected from respondents ($n = 106$) who owned and made use of a wearable device. Respondents were recruited through social media and sent a link to access the questionnaire via email. Respondents were informed of their rights and that participating in the study was voluntary and they could withdraw at any time. Ethical approval was obtained from the University of Fort Hare Research Ethics Committee, and written consent was obtained from the respondents before the completion of the questionnaire.

Results

Results from the questionnaire are summarised and presented in this section. Table 1 provides a summary of the descriptive statistics of the respondents who took part in the study as well as the information about the wearable devices that they used. The Cronbach's α score was found to be 0.832, which showed good internal consistency for the questionnaire, as suggested by Nunnally (1978). Table 2 provides an overview of the results for the privacy concerns of users of wearable devices.

More than half of the respondents (51.89%) understood that health information is sensitive or confidential in nature. More than half of the respondents (51.89%) admitted that they were not familiar with their mobile health device's information security policies and how the product

Table 3. Confidentiality–integrity–availability triad.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
(Confidentiality)I prefer that my health data be stored anonymously	47 (44.34%)	23 (21.70%)	16 (15.09%)	8 (7.55%)	12 (11.32%)
(Integrity)I worry about who has access to my health data	15 (14.15%)	21 (19.81%)	26 (24.53%)	18 (16.98%)	32 (30.19%)
(Availability)My health information must be available 100% of the time in order to be useful	26 (24.53%)	33 (31.13%)	25 (23.58%)	15 (14.15%)	7 (6.60%)

Table 4. Information security during transmission and storage.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I am aware of how my mobile health device encrypts sensitive data when transmitting to my phone or computer	19 (17.92%)	14 (13.21%)	27 (25.47%)	28 (26.42%)	18 (16.98%)
I know the types of information that is stored on or transmitted from my mobile health device	17 (16.04%)	20 (18.87%)	29 (27.36%)	23 (21.70%)	17 (16.04%)
I know whom to contact if I suspect an information security incident	15 (14.15%)	12 (11.32%)	19 (17.92%)	37 (34.91%)	23 (21.70%)
My sensitive/critical data are backed up on a routine basis and recovery is tested periodically	11 (10.38%)	20 (18.87%)	29 (27.36%)	27 (25.47%)	19 (17.92%)

provider protected their information and privacy. Lastly, 52.83% of the respondents were not familiar with how their mobile device transmitted, stored, labelled or handled sensitive information (see Table 2).

The integrity of the health data, or who had access to the data collected, was not a concern for 47.17% of respondents, while the majority of respondents (66.04%) did consider the confidentiality or anonymity of their health data to be important. More than half of the respondents (55.66%) understood that their health information must be available 100% of the time in order to be useful (see Table 3).

During transmission and storage from the wearable device to the mobile application or software program, data can also be subject to security threats. Table 4 provides an overview of these information security concerns. Just more than a third of respondents (34.91%) strongly agreed or agreed that they knew the types of information that are stored on, or transmitted to, their mobile devices, while 43.40% of respondents were not aware of how sensitive data are encrypted when transmitted to the phone or computer. Fifty-six per cent (56.61%) of respondents did not know whom to contact if they suspected an information security incident, while only 25.29% of respondents backed up sensitive or critical data routinely and tested recovery periodically.

Discussion

This study examined privacy and information security issues associated with wearable health devices. While the ability of these devices to collect and store large amounts of private information has advanced at a rapid pace, the privacy and information security concerns of the user have not kept pace with these developments. While users are empowering themselves to take a proactive role in their healthcare, the same cannot be said regarding privacy risks that are associated with the collection of personal information. In addition to supporting the literature, the findings of this study also suggested that half of the respondents did not understand that there was a need to protect their health information (Cilliers et al., 2018; Park and Drevin, 2016). There seems to be a general lack of awareness among respondents about the information security issues surrounding the data from their wearable devices. It is likely that this reflects a wider lack of knowledge about these risks throughout the general population. The example of the US military (Drape, 2018) was one where the consequences could have been significant, yet the individuals were unaware of the device's functionality and the inherent risks to which they were exposed. Similarly, two-thirds of the participants in this study did not know what types of health information were being stored or transmitted by their wearable devices, while 43.40% were not aware of how the data were being encrypted during transmission. This lack of awareness also contributed to half of the respondents not being familiar with the information security policy for their wearable device or the information security measures used to protect their data. In addition, more than half of the respondents did not know whom to contact if they suspected an information security incident. The lack of awareness about privacy issues and blind trust of the user that their data would be protected may obfuscate the liability of service providers when data breaches occur (Anaya et al., 2018; Bellekens et al., 2016; Blobel et al., 2016; Ogundele et al., 2018).

The issue of ownership of the data has been reported in the literature (Piwek et al., 2016). In this study, only a quarter of the respondents backed up sensitive or critical data routinely and tested recovery periodically. Two-thirds of respondents indicated that the confidentiality of the collected data was essential, but fewer respondents were

concerned with the integrity of the data. This could indicate that respondents were not concerned with who had access to the information, as long as they could not be identified from the data. This assumption would be supported by the notion that health information must be available in order to be useful (Fernández-Alemán et al., 2013).

Limitations of this research include that a relatively small sample size was used in this study, which means results cannot be generalised to the entire population of wearable device users. However, the study has provided valuable insight into the important topic of privacy and information security threats in this field. The convenience sampling method used to recruit respondents to complete the survey could also have introduced bias into the study. However, the call to participate was circulated widely to reach a broad range of respondents in order to minimise this bias. A further limitation of the questionnaire was that integrity of the health data only referred to access and not to the quality of data. Future research should include a more extensive study sample and investigate specific information security measures including data quality of wearable devices.

Conclusion

The major contribution of this article is the insight into users' knowledge regarding information security threats and privacy issues in the context of wearable devices. This information is useful in order to develop a higher degree of awareness and understanding of the security threats associated with wearable devices that are used to collect patient data in the healthcare industry. Moreover, this research has demonstrated that users of these devices should be educated as to how to make informed decisions when they participate in their healthcare.

Declaration of conflicting interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work is based on the research supported in part by the National Research Foundation of South Africa for the grant: Unique Grant No. 106954.

ORCID iD


Liezel Cilliers https://orcid.org/0000-0001-9493-4311

References

Adibi S (2014) *mHealth Multidisciplinary Verticals*. New York: CRC Press.

Allard T, Anciaux N, Bouganim L, et al. (2010) Secure personal data servers: a vision paper. *PVLDB* 3(1–2): 25–35.

Anaya LS, Alsadoon A, Costadopoulos N, et al. (2018) Ethical implications of user perceptions of wearable devices. *Science and Engineering Ethics* 24(1): 1–28.

Bellekens X, Nieradzinska K, Bellekens A, et al. (2016) A study on situational awareness security and privacy of wearable health monitoring devices. *International Journal on Cyber Situational Awareness* 1: 1–25.

Blobel B, Lopez D and Gonzalez C (2016) Patient privacy and security concerns on big data for personalised medicine. *Health and Technology* 6(1): 75–81.

Cilliers L, Viljoen K and Chinyamurindi W (2018) A study on students' acceptance of mobile phone use to seek health information in South Africa. *Health Information Management Journal* 47(2): 59–69.

Das AK, Pathak PH, Chuah CN, et al. (2016) Uncovering privacy leakage in cable network traffic of wearable fitness trackers. In: *HotMobile '16 proceedings of the 17th international workshop on mobile computing systems and applications*, St. Augustine, Florida, USA, 23–24 February 2016, pp. 99–104. New York, NY: ACM. DOI: 10.1145/2873587.2873594.

de Montjoye YA, Hidalgo CA, Verleysen M, et al. (2013) Unique in the crowd: the privacy bounds of human mobility. *Scientific Reports* 3: 1–5.

Drape S (2018) How data breach is inevitable in wearable devices. Available at: https://www.wearable-technologies.com/2018/08/pentagon-tells-soldiers-to-leave-wearable-trackers-at-home-when-heading-to-warzones/ (accessed 15 December 2018).

DuFour A, Lajeunesse K, Pipada R, et al. (2017) The effect of data security perception on wearable device acceptance: a technology acceptance model. In: *Proceedings of Student-Faculty Research Day, CSIS*, Pace University, 5 May 2017, pp. 1–6.

Els F and Cilliers L (2017) Improving the information security of personal electronic health records to protect a patient's health information. In: *Proceedings of information communication technology and society conference*, Umhlanga, South Africa, 9–10 March 2017.

Farnell G and Barkley J (2017) The effect of a wearable physical activity monitor (Fitbit One) on physical activity behaviour in women: a pilot study. *Journal of Human Sport and Exercise* 12(4): 1230–1237.

Fernández-Alemán JL, Carrión Señor I, Lozoya P, et al. (2013) Security and privacy in electronic health records: a systematic literature review. *Journal of Biomedical Informatics* 46: 541–562.

Filkins BL, Kim JY, Roberts B, et al. (2016) Privacy and security in the era of digital health: What should translational researchers know and do about it? *American Journal of Translational Research* 8(3): 1560.

Genuth I (2015) All in the mind. *Engineering & Technology* 10: 37–39.

Huckvale K, Prieto JT, Tilney M, et al. (2015) Unaddressed privacy risks in accredited health and wellness apps: a systematic cross-sectional assessment. *BMC Medicine* 13(1): 214.

Katurura M and Cilliers L (2017) A review of the implementation of electronic health record systems on the African continent. In *Conference Proceedings of African Computer and Information System & Technology 2017*, Cape Town, South Africa, 10–11 July 2017.

Lambiotte BR and Kosinski M (2015) Tracking the digital footprints of personality. *Proceedings of the IEEE* 102(12): 1934–1939.

Malambo P, Kengne AP, Lambert EV, et al. (2016) Prevalence and socio-demographic correlates of physical activity levels among South African adults in cape town and mount frere communities in 2008-2009. *Archives of Public Health* 74: 54.

Martínez-Pérez B, de la Torre-Díez I and López-Coronado M (2015) Privacy and security in mobile health apps: a review and recommendations. *Journal of Medical Systems* 39(1): 181–190.

Mehraeen E, Ghazisaeedi M, Farzi J, et al. (2016) Security challenges in healthcare cloud computing: a systematic review. *Global Journal of Health Science* 9(3): 157.

Meingast M, Roosta T and Sastry S (2006) Security and privacy issues with healthcare information technology. In: *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, 31 August–3 September 2006, pp. 5453–5458. New York, USA: IEEE.

Montgomery K, Chester J and Kopp K (2018) Health wearables: ensuring fairness, preventing discrimination, and promoting equity in an emerging Internet-of-Things environment. *Journal of Information Policy* 8: 34–77.

Ngamntwini B and Cilliers L (2018) A usability framework for diabetic health applications in South Africa. In: *Conference Proceedings of Future Technology Conference 2018*, Vancouver, Canada, 13–14 November 2018.

Nunnally JC (1978) *Psychometric Theory*. New York: McGraw-Hill.

Ogundele O, Isabirye N and Cilliers L (2018) A model to provide health services to hypertensive patients through the use of mobile health technology. In: *Conference Proceedings of African Conference of Information and Communication Technology*, Cape Town, South Africa, 10–11 July 2018.

Park M and Drevin L (2016) An investigation into the security behaviour of tertiary students regarding mobile device security. In: *Conference Proceedings of CONF-IRM 2016 Proceedings*, Durban, South Africa, 2016, Paper 63. Available at: http://aisel.aisnet.org/confirm2016/63 (accessed 15 December 2018).

Pearson S (2012) *Privacy, Security and Trust in Cloud Computing*. New York: IBM.

Piwek L, Ellis DA, Andrews S, et al. (2016) The rise of consumer health wearables: promises and barriers. *PLoS Med* 13(2): e1001953.

Scholz T (Ed.) (2012) *Digital Labour: The Internet as Playground and Factory*. New York: Routledge.

Seneviratne S, Hu Y, Nguyen T, et al. (2017) A survey of wearable devices and challenges. *IEEE Communications Surveys & Tutorials* 19(4): 2573–2620.

Shisana O, Labadarios D, Rehle T, et al. (2013) *South African National Health and Nutrition Examination Survey*. Cape Town, South Africa: SANHANES.

Statista (2016) Facts and statistics on wearable technology. Available at: https://www.statista.com/topics/1556/wearable-technology/ (accessed 16 September 2016).

Suna D, Chang G, Suna L, et al. (2011) Advanced in control engineering and information science surveying and analysing security, privacy and trust issues in cloud computing environments. *Procedia Engineering* 15: 2852–2856.

Tana J, Forss M and Hellstén T (2017) The use of wearables in healthcare–challenges and opportunities. Arcada Working papers. Arcada, Finland: Department of Health and Welfare. ISBN 978-952-5260-83-0.

Varadharajan V (2009) A note on trust-enhanced security. *IEEE Security and Privacy* 7: 57–59.

Westin AF (1967) *Privacy and Freedom*. New York: Atheneum.

Wolf BC, Polonetsky J and Finch K (2016) *A Practical Privacy Paradigm for Wearables*. Washington: Future of Privacy Forum. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjryIHd3f_gAhX6RhUIHZudAyMQFjAAegQICRAC&url=https%3A%2F%2Ffpf.org%2Fwp-content%2Fuploads%2FFPF-principles-for-wearables-Jan-2015.pdf&usg=AOvVaw0nqNyo0Ju0SEk4CmvezYut (accessed 13 April 2019).

Wright M (2014) The dark side of wearable tech: Should you be worried? *Brandwatch* 17 November 2014. Available at: https://www.brandwatch.com/blog/dark-side-wearable-tech/ (accessed 30 July 2018).

Zhou J, Cao Z, Dong X, et al. (2015) Security and privacy in cloud-assisted wireless wearable communications: challenges, solutions, and future directions. *IEEE Wireless Communications* 22(2): 136–144.