1-8-2019

Healthcare Equity: Questions of Access and Security

Cherie Noteboom
Dakota State University

Matthew Noteboom
University of Minnesota

1-8-2019

Healthcare Equity: Questions of Access and Security

Cherie Noteboom
Dakota State University

Matthew Noteboom

Healthcare Equity Barriers: Questions of Access and Security

Cherie Bakker Noteboom, PhD
Dakota State University
Cherie.Noteboom@dsu.edu

Matthew Noteboom
University of Minnesota
Matthewnoteboom10@gmail.com

Abstract

The rapid growth of mobile technology to improve healthcare conditions, support patient engagement, and enhance patient education is expected to continue its upward trend. Physicians feel that simplified access to health information is one of the greatest benefits of technology. This research connects the growth of patients' healthcare data access via mobile applications and the growth of access to wireless communication. This article proposes the following questions to investigate potential healthcare equity barriers: "What is the available Wi-Fi coverage?" and "What types of security protocols are used in the wireless access points?" The results indicate that there is a difference in community access to available Wi-Fi coverage. This difference could influence healthcare equity barriers. In addition, communities had identical security protocol usage. This indicates an opportunity to improve knowledge of security protocols and maintenance of access points, as well as influences on healthcare equity barriers.

1. Introduction

Healthcare organizations in the United States are investing in information technology (IT) to reduce the associated cost of services and improve the quality of patient care in a move toward population health initiatives. IT systems in healthcare organizations must meet requirements as they positively impact patients. Many of these initiatives focus on education and the engagement of the patient population. Wi-Fi-supported applications, which continue to experience great growth, are considered a key IT strategy to engage and educate the healthcare population [1,2].

Healthcare continues to integrate IT solutions to transform the methods of patient interaction to support patient engagement and education. These solutions are transforming how patients participate in their individual care. Seventy-eight percent of healthcare customers either wear or are willing to utilize wearable technology solutions to track their lifestyle choices and vital signs. Mobile medical technology is advocated by 75.5% of physicians who feel that the technology simplifies access and is one of the greatest benefits of mobile medical technology. Nearly half of hospitals provide applications (apps) for patient education and engagement; 58% of hospitals have patient portal solutions [3]. The number of health apps exceeds 165,000 [4]. The use of healthcare apps and patient portals requires consumer understanding of security protocols and awareness of access.

However, little investigation has been done to connect patients' growing mobile access to healthcare data and the value of wireless communication, security protocols, and access points. A growing number of people carry wireless devices and smartphones to communicate with each other and with central service providers. The default expectation is that wireless networks provide seamless access and secure data transmission. With the growing focus on healthcare apps and confidential healthcare data transmission, it is necessary to understand the importance of wireless network security protocols and access availability. One of the most important parameters for evaluating public space, as well as the efficiency of wireless networks, is accessibility. The second feature is security. To discover healthcare equity barriers, this research surveys access points in two midwestern communities to investigate the following questions: "What is the available Wi-Fi coverage?" and "What types of security protocols are used in the wireless access points?"

2. Background

An exponential growth of communication technologies has allowed us to reach more individuals regardless of location. In turn, new types of health interventions have emerged. Smartphones and/or mobile-based patient portals enhance patient engagement at a very low cost. Due to the promising influence of smartphone-based technologies in supporting healthy lifestyles and self-care practices, researchers have been inspired to explore the impact

URI: https://hdl.handle.net/10125/59830
ISBN: 978-0-9981331-2-6

and use of mobile applications. For example, women widely use mobile apps for health information during pregnancy. However, it is reported that apps are unavailable for postpartum information, which highlights the need for the development of more mobile apps focusing on postpartum content [5]. In another example, Zhang et al.'s [6] study is one of the few studies to describe the methodology of developing an online- and smartphone-compatible cognitive behavioral therapy intervention program for bariatric surgery patients.

Providers see positive results regarding health information technology (HIT) use with motivated users. It appears that motivated patients can achieve significant improvements in their health through mobile applications [7]. These patients have been categorized as motivated, healthy information seekers or chronically monitored patients [8]. According to a Gartner press release, worldwide mobile application downloads were expected to reach 268 billion in 2017. Apps are becoming one of the most popular computing tools across the globe. Approximately 500 million people were expected to use mobile health applications in 2015 [9].

A communication infrastructure's availability and security support rapid growth and positive health outcomes. The advent of computing and its increase in power was initially embraced by healthcare providers without much regard for technical safeguards. However, technical safeguards were developed due to increased media attention during security breaches relating to patient records and confidentiality [1]. Mobile devices, cloud computing systems, and new applications in the healthcare sector have created a distinct set of challenges for those involved in data and/or information security [10].

Wireless technologies are categorized depending on their function, frequencies, bandwidth, communication protocol, and level of sophistication [11]. Wi-Fi, which facilitates an ease of use, is standard communication in homes and businesses. Multiple Wi-Fi access points are frequently located in these areas. Wi-Fi security issues continue to be a problem as the number of access points grows. Security concerns exist because Wi-Fi users may be uninformed and unaware of underlying security weaknesses. This may be due to an unfamiliarity or unawareness of security protocols and lack of knowledge of accepted Wi-Fi security standards. Meanwhile, malicious individuals actively hunt for nonsecure Wi-Fi access points as they attempt to gain unauthorized access to networks. As the importance of Wi-Fi security has been stressed in mass media, the assumption is that users are aware of the need to secure these access points. However, users may lack the knowledge to distinguish between a poorly configured point and a reasonably secure access point. This is an area of concern due to increasing reliance on access points and constant connections by smart phone users and healthcare apps. The average user must understand security protocols in their infrastructure.

Security protocols include wired equivalent privacy (WEP), Wi-Fi protected access (WPA), and 802.11i (WPA2). WEP is an encryption algorithm developed by the IEEE volunteer group. However, some flaws make WEP crackable as individuals can sniff information from the airwave and learn the first three characters of the secret key [12]. WEP has widely known and exploited encryption weaknesses. Tools exist that automate the process of cracking WEP security. Technical expertise is not required to exploit WEP. Therefore, WEP is now infamous for providing a false sense of security. When asked, users who deploy WEP to secure their access points were found to be unaware of the inherent weaknesses associated with it. In addition, these users have not upgraded their security. Breaking WEP security is not a matter of whether it can be done. It is a matter of how quickly it can be done.

WPA was created as an intermediate solution to correct WEP weaknesses. It patched WEP problems using a software upgrade. However, it introduced two additional faults. This second-generation security mechanism aims to provide reliable communication is 802.11i or WAP2, as well as additional protections to Wi-Fi. However, it requires a careful setup and protection. Otherwise, it can suffer from successful hacking attempts [13].

3. Methodology

This research conducts a survey of wireless access points in two midwestern communities. The communities were selected based on varying socioeconomic and demographic data found in the available census data. The communities have variation in economic indicators and demographic information. The communities are both served by two large healthcare organizations serving the midwestern region. The healthcare organizations are actively engaged in the deployment of healthcare apps, improvement of health care quality and the engagement of patients in mobile apps for management of care and wellness.

According to census data, the community one selected for this survey investigation had a population of 1,911 people (93.7% white). Community two

Economics	Community One		Community Two
Population	1,911		847
Estimated Per Capita Income	$30,726		$15,955
Average House Value	$161,611		$46,919

represents a midwestern Indian reservation with census data specifying a population of 847 people (52.7% American Indian, 40.8% white) [14].

The economic data for the two communities is presented in Table 1 and indicates significant differences in estimated per capita income and average home value.

Table 1. Economic data

The goal is to investigate wireless networking from an access coverage and security protocol perspective. It aims to determine whether the two communities have similar Wi-Fi coverage and security protocols to support the growth of healthcare apps. It also reviews the potential to support equitable healthcare app use to positively influence health outcomes. The data collection utilizes "wardriving" to collect wireless access point information. The data is analyzed to determine security protocol usage and access point availability. The results are evaluated and presented with a visualization of the access point protocol usage and access point distribution. This research posts the following questions to investigate potential healthcare equity barriers: "What is the available Wi-Fi coverage?" and "What types of security protocols are used in the wireless access points?"

This research utilized the wardriving data gathering method. Popularized in 2001, this method gathers information on the number of access points. Next, it assesses and/or categorizes the security level of access points in a typical, midwestern community. Individuals, usually in a moving vehicle, execute the war hunting method as they search for Wi-Fi access points. The intent of the wardriving activity can vary. Some efforts pursue this activity for security research purposes. Others do it to gain illegitimate access to poorly secured wireless networks. The interest in wardriving has increased as the number of access points has grown [11].

The entire community was targeted for data collection during the study. The effort required: (1) an Android device; (2) a WiGLE Wi-Fi app; (3) a computer with Python programming language; and (4) Google application programming interface (API). The Android device with the WiGLE Wi-Fi app collected data from each access point. The app, which was available on Google Play, is described as an open-source wardriving app to NetStumbler. It displays and maps detected wireless networks and cell towers throughout the world. Information is easily uploaded to the WiGLE database (https://wigle.net/). WiGLE, started in 2001, has more than 250 million Wi-Fi networks worldwide [15]. The Python programming language exported keyhold markup language (KML) files on a secure digital (SD card) to import to Google Maps. The Google API completed the interactions to map the coordinates and create heat maps for analysis and visualization.

The data collection vehicle and equipment moved slowly through the community's streets. Data collection in community one took 4 hours and 36 minutes. Collection in community two took 4 hours and 16 minutes. Data was collected from 1,286 Wi-Fi access points in community one and 491 access points in community two. Penetration and/or cracking was not performed during the research.

4. Results and Analysis

Wireless access points provide access to apps like streets provide access to public spaces. The research goal aimed to answer the following questions to investigate potential healthcare equity barriers: "What is the available Wi-Fi coverage?" and "What types of security protocols are used in the wireless access points?"

Table 2. Security protocols community one

Encryption	Number	Percentage
None	193	15%
WEP	13	1%
WPA/WPA2	1,080	84%
Totals	1,286	100%

For community one, 1,286 wireless access points were discovered by scanning the entire community. Of the access points analyzed, 15% had no encryption, 1% utilized outdated WEP, and 84% utilized WPA or WPA2. Table 1 summarizes the results. Eighty-four percent of the access points utilized WPA or WPA2 security protocol. Sixteen percent, which were

comprised from no encryption and WEP security protocol, present an opportunity for upgrades. Access points on older, flawed versions of security protocols offer an opportunity for increased awareness and education on installation, upgrades and maintenance.

The data was downloaded as a KML file. Python was used to parse the network coordinates. A heat map was created using Google Maps API to visualize the concentrations and availability of access points throughout the town. Analysis of the latitude and longitude of locations collected from the access points was analyzed with the Python program to parse the network coordinates. The sample code is listed in Figure 1.

```
export.py - C:\Users\matth\Desktop\Heatmap_package\export.py (2.7.13)
File  Edit  Format  Run  Options  Window  Help
import pykml
from pykml import parser

import argparse

argparser = argparse.ArgumentParser(description="Tool built to scrape KML files

argparser.add_argument('-f', '--file', help='KML file to scrape for coords')
argparser.add_argument('-o', '--output', help='Filename to output to')

args = argparser.parse_args()

if not (args.file):
    print("[!] No input file specified.")
    exit()

if not (args.output):
    tmp = args.file.split('.')

    dest = str(tmp[0]) + '_edited'
else:
    dest = "coords_edited"

root = parser.fromstring(open(args.file, 'r').read())
```

The heat map in Figure 2, which displays community one, indicates the greatest concentrations of access points in the business district and K-12 community school district. However, the community appears to have consistent access throughout the neighborhoods indicating access for the community neighborhoods. The path travelled to collect the data is visible. The portion of the community without roads or heat map colors is the golf course.

Table 3. Security protocols community two

Encryption	Number	Percentage
None	74	15%
WEP	5	1%
WPA/WPA2	412	84%
Totals	491	100%

For community two, there were 491 access points discovered by scanning the community. Of the access points analyzed, 15% had no encryption, 1% utilized outdated WEP, and 84% utilized WPA or WPA2. Table 2 summarizes the results. Eighty-four percent of the access points utilized WPA or WPA2 security protocol. Sixteen percent, which were comprised from no encryption and WEP security protocol, presents an opportunity for upgrades. Access points on older, flawed versions of security protocols offer an opportunity for increased awareness and education on installation, upgrades and maintenance.

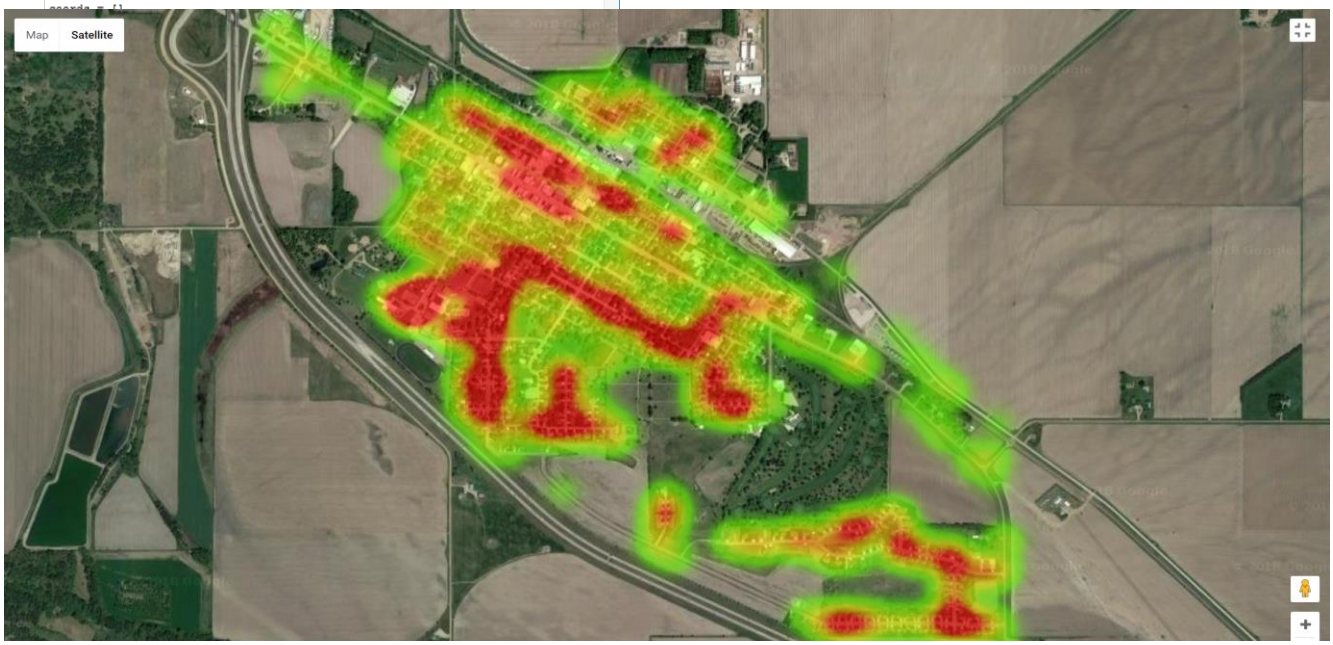

Figure 2. Heat map community one

When neglected, poorly configured Wi-Fi access points act as facilitators of malicious intent. With more people relying on Wi-Fi to access their healthcare apps and sensitive data, security is a key issue. Table 1 shows that 15% of the access points did not utilize encryption; 1% remained on the weak WEP protocol. These categories of access points would benefit from review and enhancement of their configurations. Analysis of security protocol data revealed an opportunity to tackle the issue of outdated security protocol utilization.

The data was downloaded as a KML file. Python was used to parse the network coordinates. A heat map, which was created using Google Maps API, visualized the concentrations and availability of access points throughout the town. Analysis of the latitude and longitude locations collected from the access points was analyzed with the Python program to parse the network coordinates.

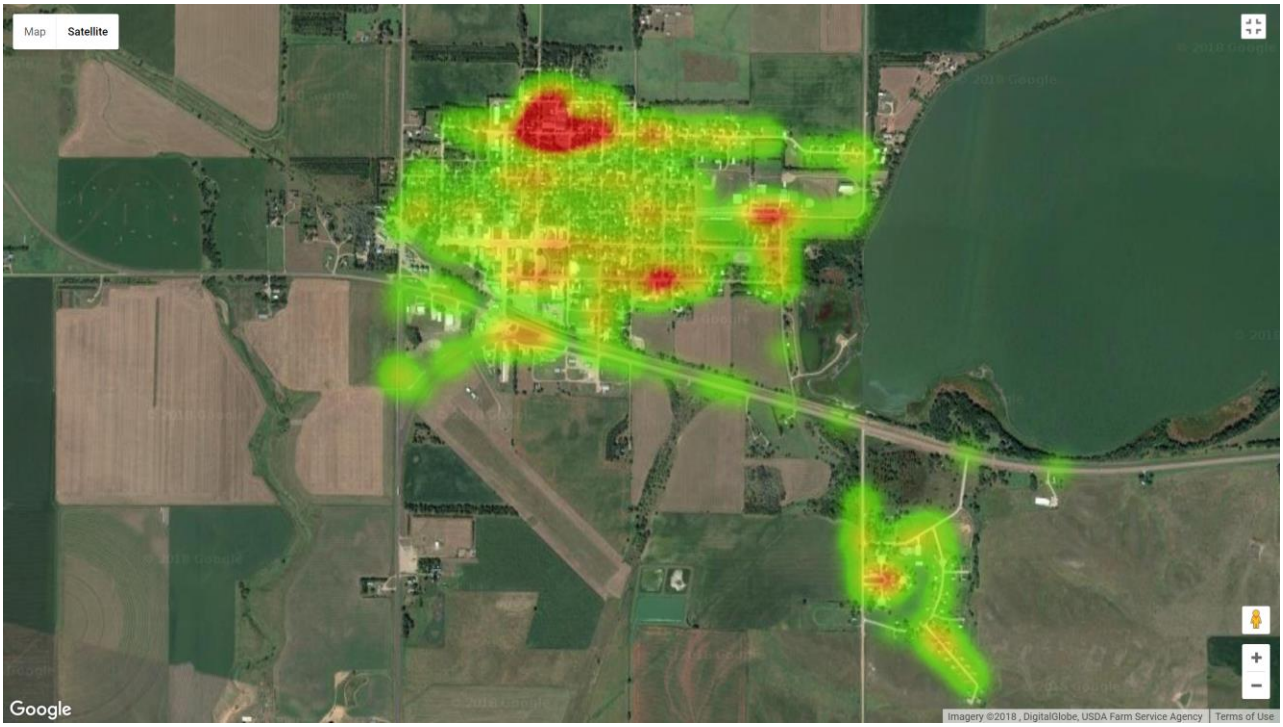

Figure 3. Heat map community two

The heat map in Figure 3 indicates the greatest concentrations of access points in the federal government offices, hospital, healthcare facilities and K-12 community school district. There are very few concentrations of access in the residential community areas or the federal housing developments.

The comparison of the two communities does point out variation in access which could lead to disparities of access to health care and wellness tools and support. Community One has consistent concentrations of access throughout the community and the residential areas. Community Two's heat map indicates less access throughout the residential areas. The reasons for the difference may be related to the community selection criteria. The selection of the communities was based on the differences in economic indicators and demographic data. These differences could influence the variation of access. The community with the lower economic indicators, community two, has less access in the residential areas. This indicates potential for less access for individual residents. Both communities appear to have access concentrations in their business district and their K12 School District areas. Community Two, a federal Indian reservation, has the additional access concentration in the federal offices and hospital property. Community two's location on the Indian Reservation may influence the concentration of access in these areas. It is unclear how this concentration may influence the accessibility of access points or services to residents. Further research needs to be completed to further investigate the differences to resident's access.

This study has limitations due to the limited number of communities explored, the limited number of factors investigated and the lack of information regarding specific health conditions of the

communities' residents and the health care apps utilized by the residents of the communities.

5. Conclusion

From a public health perspective, patient-centered care requires "a partnership among practitioners, patients, and their families (when appropriate) to ensure that decisions respect patient's wants, needs, and preferences and that patients have the education and support they need to make decisions and participate in their care" [16, p. 7]. There is a concentrated effort to provide patient engagement and patient education through Wi-Fi communication channels. Healthcare organizations have built their IT infrastructures with an intentional regard for the security of patient data. The last link to the patient appears to be the weak link.

This research indicates a disparity of access between community one and community two. The disparity of access has the potential to be a barrier to healthcare equity supported by Wi-Fi access and healthcare apps. A secondary finding indicates a lack of understanding of security protocols by typical residents of both midwestern communities. The need to maintain and upgrade access points appears to be a missed opportunity. This research indicates that security protocols may be a neglected component of access. The 16% of users with WEP or no encryption would benefit from attention and maintenance to their current access solutions.

For the future, it is difficult to see anything other than refinements and growth of current healthcare strategies to utilize technology to improve patient engagement and support [17,18] The expansion of patient portals, chronic disease apps, and educational tools to support patients are expected to grow at increasing rates [19,20]. Use of connected health solutions are becoming standard practice among hospitals in the U.S. as 81% of hospitals leverage this type of IT [3].

According to a 2016 HIMSS survey, 47% of respondents emphasized personal technology to influence patient satisfaction, treatment monitoring, patient engagement, and patient education. These individuals planned on continuing to grow in these areas [3]. This study discovered a barrier to implementation due to inequitable access to infrastructures.

As technological advances continue, the established user base may lag in updating existing systems. The invisibility of infrastructure and communication items, such as security protocols and access points, enable the user to continue use without realizing the need for maintenance. Healthcare stakeholders agree that it is important to maintain public confidence in the healthcare sector. There is comprehensive support for the rights currently afforded to patients [1,21]. In contrast, the technical safeguards in the healthcare industry will become transparent. There will be greater sophistication regarding both hardware and software. Yet there will be less to see because successful technical safeguards are invisible [1].

This research provides insight to healthcare practitioners as they implement and support HIT applications to patients. There is a need to increase awareness of the invisible components of IT. In addition, there is a need to increase education regarding minimum maintenance of the hidden solutions. As we overcome the challenges of providing access to the "last mile," we may realize that the second challenge is the necessary "maintenance of the last mile." Sustained attention and education on the invisible components of our infrastructure will be necessary to prevent access and security gaps. Overcoming these challenges is just the beginning. The next level will include maintenance. This research identifies a potential source of healthcare barriers and inequity of care support between two communities.

Future research is necessary to expand the survey beyond two midwestern communities. There is a need to explore the healthcare application utilization and healthcare status of the communities under study. It would also be beneficial to survey users to evaluate their level of security awareness.

6. References

[1] T.Z. Allan and Y. Wang, "The Demand for Technical Safeguards in the Healthcare Sector: A Historical Perspective Enlightens Deliberations about the Future", In Proceedings of Americas Conference on Information Systems, 2017.

[2] J. A. Sacristán, "Patient-Centered Medicine and Patient-Oriented Research: Improving Health Outcomes for Individual Patients", BMC Medical Informatics and Decision Making, London, 2013, p. 6.

[3] Institute of Medicine (IOM), "Envisioning the National Health Care Quality Report", The National Academies Press, Washington, DC, 2001.

[4] Microsoft, "Engage Your Patients", Infographic, Retrieved from http://pages.healthcareitnews.com/rs/922-ZLW-

292/images/Engage%20your%20patient%20infographic.pdf?aliId=678046187

[5] L. Guerra-Reyes, V.M. Christie, A. Prabhakar, A.L. Harris, and K.A. Siek, "Postpartum Health Information Seeking Using Mobile Phones: Experiences of Low-Income Mothers", Maternal and Child Health Journal, Springer, New York, 2016, pp. 13-21.

[6] M.W. Zhang, R. Ho, S.E. Cassin, R. Hawa, and S. Sockalingam, "Online and Smartphone Based Cognitive Behavioral Therapy for Bariatric Surgery Patients: Initial Pilot Study", Technology and Health Care, European Society for Engineering and Medicine, Copenhagen, 2015, pp. 737-744.

[7] J.M. García-Gómez, I. de la Torre-Díez, J. Vicente, M. Robles, M. López-Coronado, and J.J. Rodrigues, "Analysis of Mobile Health Applications for a Broad Spectrum of Consumers: A User Experience Approach", Health Informatics Journal, Sage, 2014, pp. 74-84.

[8] H. Fraser, Y. Kwon, and M. Neuer, The Future of Connected Health Devices, IBM Institute for Business Value, Armonk, NY, 2011.

[9] J. Rodriguez, I. Lopes, and B. Silva, "A New Mobile Ubiquitous Computing Application to Control Obesity: SapoFit", Informatics for Health and Social Care, Taylor and Francis Online, Abingdon, 2013, pp. 37-53.

[10] C. Bhatt, M.Chintan, and S. Peddoju, Cloud Computing Systems and Applications in Healthcare, IGI Global, Hershey, PA, 2017.

[11] H. Berghel, "Wireless Infidelity I: War Driving", Communications of the ACM, New York, 2004, pp. 21-26.

[12] SANS Institute, "The Evolution of Wireless Security in 802.11 Networks: WEP, WPA and 802.11 Standards", SANS Institute Information Security Reading Room, 2003.

[13] V. Kumar, A. Tiwari, P. Tiwari, A. Gupta, and S. Shwawne, "Vulnerabilities of Wireless Security Protocols", International Journal of Advanced Research in Computer Engineering & Technology, New Chouksey Nagar, 2012.

[14] American FactFinder, United States Census Bureau. Retrieved June 6, 2017 from https://factfinder.census.gov/faces/nav/jsf/pages/index.xhtml

[15] Google Play, WiGLE WiFi Wardriving, Retrieved June 8, 2017 from https://play.google.com/store/apps/details?id=net.wigle.wigleandroid

[16] Institute of Medicine, Committee on Health Care in America (IOM). (2001). Crossing the quality chasm: A new health system for the 21st Century. Washington, DC: National Academy Press.

[17] G.C. Kane and G. Labianca, "IS Avoidance in Health-care Groups: A Multilevel Investigation", Information Systems Research, Maryland, 2011, pp. 504-522.

[18] B. Cliff, "Using Technology to Enhance Patient-Centered Care", Journal of Healthcare Management, American College of Healthcare Executives, 2012, pp. 301-303.

[19] S.B. Cohen, K.D. Grote, W.E. Pietraszek, and F. Laflamme, Increasing Consumerism in Healthcare Through Intelligent Information Technology", The American Journal of Managed Care, New Jersey, 2010, pp. SP37-43.

[20] S. McAlearney, C.J. Sieck, J.L. Hefner, A.M. Aldrich, D.M. Walker, M.K. Rizer, et al., "High Touch and High Tech (HT2) Proposal: Transforming Patient Engagement Throughout the Continuum of Care by Engaging Patients with Portal Technology at the Bedside", JMIR Research Protocols, Canada, 2016.

[21] K.J. O'Leary, R.K. Sharma, A. Killarney, L.S. O'Hara, M.E. Lohman, E. Culver, et al., "Patients' and Healthcare Providers' Perceptions of a Mobile Portal Application for Hospitalized Patients", BMC Medical Informatics and Decision Making, London, 2016, p. 123.