6-2018

Patient Preferences for Authentication and Security: A Comparison Study of Younger and Older Patients

Ann Fruhling
University of Nebraska at Omaha, afruhling@unomaha.edu

Devika Ramachandran
University of Nebraska at Omaha, dramachandran@gmav.unomaha.edu

Tamara Bernard
University of Nebraska Medical Center, tbernard@unmc.edu

Ryan Schuetzler
University of Nebraska at Omaha, rschuetzler@unomaha.edu

John R. Windle
University of Nebraska Medical Center

Patient Preferences for Authentication and Security: A Comparison Study of Younger and Older Patients

Ann Fruhling[1], Devika Ramachandran[1], Tamara Bernard[2], Ryan Schuetzler[1], John Windle[2]
[1]University of Nebraska Omaha, Omaha, Nebraska, 68182, USA,
afruhling@unomaha.edu, dramachandran@unomaha.edu, rschuetzler@unomaha.edu
[2]University of Nebraska Medical Center, Omaha, Nebraska, 98198-2265, USA, tbernard@unmc.edu, jrwindle@unmc.edu

ABSTRACT

We examine authentication and security preferences of younger versus older patients in the healthcare domain. Previous research has investigated users' perception of the acceptability of various forms of authentication in non-healthcare domains, but not patients' preferences. First, we developed an interactive prototype to test three authentication methods: passwords, pattern, and voice. Our results indicate that younger patients prefer passwords by a significant margin. Older patients indicated more mixed preferences. In addition, we evaluated the level of security patients desired for protection of health information compared to financial information. We found no difference based on age: both groups felt financial security is more important than health data security. The findings of this research can be used to improve and enhance usability of future PHRs and overall PHR usage by patients. While this study is specific to cardiology patients we believe the results are generalizable to all patients with chronic conditions.

ACM Reference format:

Ann Fruhling[1], Devika Ramachandran[1], Tamara Bernard[2], Ryan Schuetzler[1], and John Windle[2] 2018. Patient Preferences for Authentication and Security: A Comparison Study of Younger and Older Patients. In Proceedings of ACM SIGMIS-CPR'18, Buffalo-Niagara Falls, NY, USA, June 2018, 7 pages. https://doi.org/10.1145/3209626.3209702

CCS Concepts

• Security and privacy~Authentication • Human-centered computing~Empirical studies in interaction design

KEYWORDS

PHRs; usability; authentication; privacy; security; prototype; patients; cardiology

SIGMIS-CPR '18, June 18–20, 2018, Buffalo-Niagara Falls, NY, USA

ACM ISBN 978-1-4503-5768-5/18/06.
https://doi.org/10.1145/3209626.3209702

INTRODUCTION

Patient authentication to access personal health records (PHRs) is mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) due to the sensitive nature of health information [18]. Health information includes identifiable information about the patient's health conditions, contact information (name, address, telephone number), and other personal information (insurance policy number, credit card number, banking information, etc.) that may be linked to their finances. In computing, authentication is the process of verifying the identity of the person attempting to access a resource [26]. In the case of PHRs, it is used to verify a patient's identity before allowing access to his or her health information.

Although a username (unique identifier) and password combination is the most common authentication method used to access PHRs [3], the difficulty of remembering a username and password was a frequent complaint by patients in a recent study of the wants and needs of patients using PHRs [5]. Alternative authentication methods such biometric scans (e.g., fingerprint, face, voice, or retina), token-based authentication, recognition-based graphical password techniques [23], and login through email notification [16] could remedy this problem. When implementing new technology—including novel authentication techniques—it is important to evaluate how users, in this case patients, perceive the new technology and the likelihood of acceptance.

BACKGROUND

HITECH

The 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act placed new requirements on health care organizations in terms of Meaningful Use criteria which drive reimbursements from the US government for patient-centered care [17]. Meaningful use Stage 1 focuses on data capture and sharing. Stage 2 focuses on advanced clinical processes such as health information exchange and increased patient-controlled data. Increasing PHR usage is required to achieve Stage 2 [19].

Health organizations are motivated to continue to offer more features in their patient portals [25] due to governmental pressure to meet the Meaningful Use Stage 2 requirement,. They recognize that patients have an increased interest and desire to securely message with their care providers as well as to actively manage and monitor their diseases. The ability for patients to view their health information electronically meets the Meaningful Use Stage 2 requirement.

Older Adults

Older adults are poised to be the fastest growing patient group of PHR users. Due to smart phones and social media such as Facebook older adults appear to be interested in investing time in learning needed computer skills. Further, older adults often have a higher need to access online health information than younger adults. Older adult populations, when compared to younger adult populations, have a higher proportion of having some type of disability. According to the Administration on Aging (2002) 44.5% of older adults ages 65-69 have a disability, and this increases to 73.6% for those 80 years and older [1]. Chronic disabilities (e.g. arthritis, hearing impairments, cataracts, hypertension, heart disease, and diabetes) are the leading types of disabilities. Older adults are also more likely to be in regular contact with a healthcare professional than younger adults, with 86% of adults aged 65-74 reporting contact with a healthcare professional in the last six months, compared with 59% for adults age 18-44 [8].

Many older adults are realizing the Internet provides immediate access to a wealth of health information and resources that might not otherwise be available. On the other hand, accessing these health resources and understanding how to find the information can be more of a challenge for older adults due to aging, lower education, and unfamiliarity with technology.

Older adults tend to face more barriers than younger adults in terms of eyesight, memory, and computer self-efficacy. Key website usability factors identified for older adults were vision, cognition, and motor skills. Becker (2004) assessed 125 websites evaluating usability barriers that impact older adult users. In their study they identified several barriers including: pull-down menus and small font size impacting readability, screen length increasing cognitive load, and missing help features such as contact us, privacy statement, and site maps [6].

Toscos et al. (2016) found a "novelty effect" in the level of continual patient usage of PHRs [33]. Patients' interest in PHR usage started out high because it was something new and then their interest and usage declined. Toscos et al. (2016) also noted PHR training and age as factors of usage. In their study, the authors reported older adults were more likely to be super users and utilized the PHR more often. However, older adults self-reported their computer and Internet abilities being lower than younger adults. In another study, Chrischilles et al. (2014) found older adults were especially interested in tracking their medication and health information [12].

Patient Health Records

For most healthcare organizations, increasing patient engagement and patient activation is a universal healthcare goal. One of the first steps to patient activation is accessing the PHR. PHRs provide an important communication avenue between healthcare providers and patients [34]. Patients who use PHRs report several positive effects such as knowing more about their health care, more communication with their providers, and taking more steps to improve their health such as actively monitoring their health and care by emailing or messaging their providers [29, 34]. In a systematic review on which conditions (e.g. asthma, diabetes, fertility, glaucoma, HIV, hyperlipidemia, and hypertension) were potentially sensitive to the PHR as an intervention Price et al. (2015) reported a need for more studies on how PHRs are designed, what features they have and how they are adopted [28]. Engaging more patients to use PHRs are likely to have important public health benefits [24].

Authentication

Authentication is a concept complementary to identification. When authenticating with a computer system, users (patients) must first identify who they are claiming to be. Typically, identification is done with a username. After identification, users must then take steps to prove their identity. These steps are known as authentication.

Authentication takes three primary forms: something a user *knows*, something a user *has*, or something a user *is* [36]. Each form has advantages and limitations.

The first form, *something the user knows*, typically refers to the most common form of authentication: the password. It might also refer to other secret-based authentication methods such as the PIN used in ATMs, or the pattern frequently used on Android phones [20]. There are also knowledge-based authentication methods such as cognitive questions, most commonly seen as security questions [21]. While very widespread, these forms of authentication are not without their problems. Users, for example, frequently reuse passwords or PINs [22], share passwords with others, or choose poor passwords that provide little security [7, 9]. Passwords have an advantage in user acceptance, however. Through widespread exposure over decades, passwords have become the *de facto* standard for authentication [36].

The *something the user has* factor includes such authentication factors as smart cards and authentication tokens that authenticate based on possession [36]. This form of authentication might frequently be seen for authorizing building access, but is less common as the sole factor of authentication for a computer system. However, it has become more common for sites to use the possession factor to supplement knowledge-based authentication like a password. For example, many popular websites (e.g., Gmail, GitHub, and Facebook) allow users to use two-factor authentication combining passwords and a message or unique code sent to a smartphone. In this case, the user *has* a phone and *knows* a password, providing two forms of authentication to log into the site.

The final factor included in most descriptions of authentication types is *something the user is*. This factor typically refers to biometric authentication, including through methods such as fingerprint, iris, retina, face, and voice recognition. Biometrics are often proposed as an answer to the weaknesses of secret-based authentication. Some of the biggest challenges to the adoption of biometric authentication is user acceptance [22]. Users may fear the privacy implications of having their biometric information gathered and stored [11], or they might not feel they are acceptable and useful in a given application [22]. In addition, biometrics face technical issues—

such as accuracy and scalability—not present in other traditional means of authentication.

While previous research has investigated users' perception of the acceptability of various forms of authentication in a variety of domains [11], we are the first to look exclusively at *patients'* authentication preferences in a healthcare domain. We are also the first to examine age as a moderating factor influencing authentication preferences. It is important to understand user preferences in security, as well as the perceived security associated with various authentication methods. When users believe a site is well designed for security, they have a greater sense of trust in the security of their data [32].

Our study examines patients' authentication method preferences and the preferred security level protection for health versus demographic/financial information. We compare three authentication methods: password, pattern, and voice. We also examine the influence of demographic factors such as age, gender, current PHR usage on individual security risk tolerance. Patients rated each authentication method's usability, which is defined according to ISO 9241-11, as "The effectiveness, efficiency and satisfaction with which specified users achieve specified goals in particular environments [21]."

METHOD

Although there are many potential authentication methods, not all of them satisfy security policies required in the healthcare environment. To determine acceptable authentication methods, the research team met with a Chief Security Officer at a large university medical center. In addition to the standard username/password combination, voice recognition, pattern recognition, and fingerprint were identified as acceptable authentication alternatives. For our study, we compared three methods of authentication: password, pattern recognition, and voice recognition. These authentication methods were selected because they are commonly available on smart phones and tablet computers.

Participants - Patients

Our study focused on cardiovascular patients who access their PHRs on a routine basis to manage their health care because of their chronic (ongoing) illness. We chose to study patients with cardiovascular disease because of the large impact that cardiovascular disease has on healthcare in the US and around the world. According to the American Heart Association's 2017 Heart Disease and Stroke Statistics Update, cardiovascular disease accounts for over 800,000 deaths in the US, which is equivalent to about 1 in every 3 deaths. Heart disease remains to be the number one cause of death in the US. It was estimated that about 92.1 million American adults are living with a form of cardiovascular disease or the after-effects of a prior stroke. Combined direct and indirect cost of cardiovascular disease and stroke amounts to about $316 billion [4].

Recruitment and Study Methodology

A convenience sample of diverse patients were recruited at the time of their regularly scheduled clinic appointment. At the onset of the session, the patient was asked to 1) create a username and password, 2) save a pattern with a minimum of nine dots, and 3) audio record a passphrase. Next, the patient was presented the following scenario:

> *"You have completed your follow-up visit with your cardiologist at University Medicine. The next day you would like to take a look at your updated current medications and also view your lab test results that your physician had ordered during the visit. In order to access this information, you will need to access your patient health record (PHR)."*

Subsequently, the patient was asked to use each authentication method to access the PHR prototype. The order of the authentication methods was randomly assigned to prevent bias. The PHR prototype also included other functionalities, but the patients were only required to gain access to the PHR.

A usability survey was presented to the patient after each authentication method was tested. The usability survey was derived from the System Usability Scale [10] and Weir's scale [35]. At the completion of the authentication exercise, the patients completed a survey that measured the authentication preferences, PHR usage, gender, age and the patient's desired security protection of health information and financial information. All study protocols were reviewed and approved by the university's IRB.

User Profile Setup Guidelines

We researched several sources on the best practices for pattern recognition and password creation [5, 30, 31]. The following rules were given to the patients to setup their login profile.

For Pattern Recognition the unlock pattern has 9 dots on the screen organized in a 3×3 matrix. To login using pattern recognition, a pattern has to be drawn on the screen, connecting certain points in a certain order. The rules for setting up pattern recognition are:

- At minimum, 4 dots must be used.
- At maximum, 9 dots can be used.
- Each dot can be used only once.
- The order in which the dots are connected matters (thus making it a directed graph).
- Dots are connected with a straight line meaning that all points on the path of the line get connected.

For alphanumeric passwords, the unlock screen requires entering an alphanumeric password (numbers, letters, and symbols). The rules for setting up an alphanumeric password are:

- Must be at least 8 characters in length.
- Use a combination of at least one uppercase character (A through Z) and at least one lowercase character (a through z).
- Use at least one digit (0 through 9).
- Use at least one non-alphabetic character (~!@#$%^*&;?.+_).

For voice recognition, the prototype simulated recording the patient's voice. The patient was asked to say this statement: "This is my voice password".

PHR Wireframe Prototype

An interactive PHR wireframe prototype with a user interface for each authentication method was developed for a tablet computer. Figures 1, 2 and 3 are the wireframes created for the patients to setup their user profile. Each patient was given a tablet computer to use during the study.

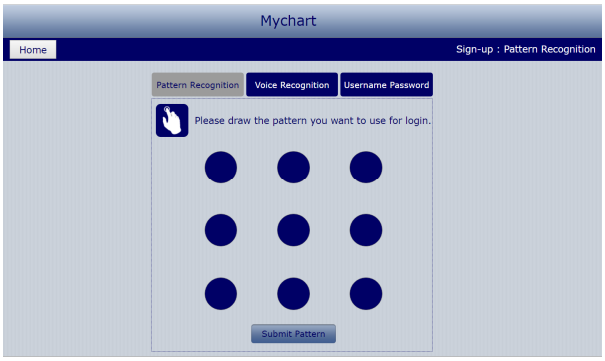

Figure 1. Setup Pattern Recognition Wireframe.

Figure 2. Setup Voice Recognition Wireframe.

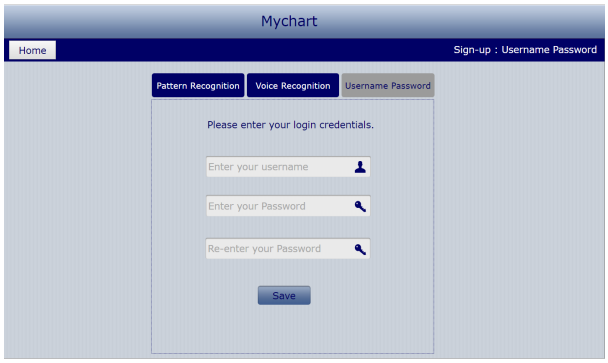

Figure 3. Setup Password Login.

Survey Development

The System Usability Scale (SUS) [10] is a commonly used light-weight, reliable tool for measuring user interface usability. SUS was selected for this study because it is easy to administer, scalable, and clearly distinguishes between high and low usability in user interfaces. After reviewing the ten SUS questions it was determined three of the questions relating to system integration did not directly apply; these questions were not included.

The survey questions that assessed the patient's preference on the level of security desired for protection of patient health information and personal financial information aligned with the definitions for security levels established by NIST 800-122 (National Institute of Standards and Technology) [27]. The levels of security are:

- **None**: No login security protection required for the data.
- **Low**: Low security level is used for the protection of low risk data.
- **Low risk data**: The loss of confidentiality, integrity, or availability of the data would have no adverse impact on your mission, safety, finances, or reputation.
- **Moderate**: Moderate security level is used for the protection of moderate risk data.
- **Moderate risk data**: The loss of confidentiality, integrity, or availability of the data could have a mildly adverse impact on your mission, safety, finances, or reputation.
- **High**: High security level is used for the protection of high risk data.
- **High risk data**: The loss of confidentiality, integrity, or availability of the data could have a significant adverse impact on your mission, safety, finances, or reputation.

RESULTS

Patient Statistics

Thirty-six patients participated in our study. Two were removed for failing to complete the survey correctly. This left 15 females and 19 males in the study. Twenty-three (68%) were under 65 and eleven (32%) were 65 and over. Sixteen (50%) indicated that they were currently using their PHR, while sixteen (50%) reported not being current users (two people failed to answer this question). Of those who reported using the PHR, 13 (81%) indicated they used their PHR at least once a month, with only 3 (19%) reporting less frequent use. Usability items for password (α=.93), pattern (α=.92), and voice recognition (α=.94) were found reliable.

Preference Ranking

In our study 22 (64.7%) of the patients ranked password as their first choice, five (14.7%) preferred voice and seven (20.5%) preferred pattern. Pattern recognition ranked second for most patients (59%), with voice recognition last (59%).

A repeated measures linear model showed a statistically significant difference ($\chi 2(2) = 9.88$, $p = .007$) in rated usability between password (M = 1.92, SD = 0.57), pattern (M = 2.20, SD = 0.74), and voice (M = 2.26, SD = 0.78) authentication methods

(in this case, a lower score indicates higher usability). A planned orthogonal contrast between password and other methods revealed that password has significantly higher usability than pattern and voice (b = .11, t(65) = 2.93, p s= .005). There was no significant difference in usability between pattern and voice authentication (b = -.09, t(65) = -1.29, p = .20). Seventeen patients (50%) indicated their preferences were in the following order: (1) password, (2) pattern, (3) voice.

Age

A linear mixed effects model with ranking as a repeated measure showed that there was a marginally significant interaction effect between the ranking of authentication types and age ($\chi 2(3) = 7.56$, $p = .056$) and no significant interaction between authentication preference and current PHR usage ($\chi 2(3) = 3.54$, $p = .32$). A post hoc analysis of mean rank indicates that younger patients prefer passwords by a significant margin. Older patients indicated more mixed preferences, with password authentication showing the best mean rank, but by a much smaller margin than for younger patients (see Table 1).

Table 1. Mean rank of authentication type by age group

	Age	
Authentication Type	**<65**	**>=65**
Password	1.30	1.91
Pattern	2.13	2.09
Voice	2.57	2.00

Post hoc analysis of the mean ranking of authentication preference for PHR users versus non-users indicated a difference not in the order of the preferences, but in the strength of those preferences. Current PHR users indicated a strong preference for password authentication, with pattern and voice showing lower ratings. For non-users, the preferences are not as strong, but the mean ranks fall in the same order of password first, followed by pattern, then voice (see Table 2).

Table 2. Mean rank of authentication type by PHR usage

	Currently using PHR?	
Authentication Type	**Yes**	**No**
Password	1.31	1.69
Pattern	2.19	2.00
Voice	2.50	2.31

Security

In general, patients wanted their data to be secure. For financial data, 32 of 34 patients indicated they wanted the highest level of security ($M = 3.91$, $SD = 0.38$). For health information, 20 of 34 wanted the highest level ($M = 3.44$, $SD = 0.79$). The results of an ordinal logistic regression [2] show a statistically significant difference between security preferences for financial and health data ($b = 2.38$, $t = 2.95$, $p = .003$), with people showing stronger preferences for security of their financial data.

DISCUSSION

The basic question we seek to answer with this research is this: what authentication method do patients prefer for accessing their PHR? The approach we took was to perform within-subjects comparisons allowing patients to rank their preferences for authentication with the system. The data for younger patients (under 65) tells a clear story: password is by far the most preferred option, followed by pattern, and finally voice. Despite the problems of having to remember a username and password, it is still the most preferred authentication method and reported the highest perceived usability. This finding may be due to the younger patients' familiarity with this method and its alignment with the authentication method commonly used for accessing other internet applications (e.g. online banking, online shopping, etc.). A few of the patients commented that they save the password for logging into the PHR on the login page which lets them login without having to remember or type it in every time they visit the site. Since some of the patients have found a way to use the password login method without needing to remember the password, they are quite comfortable with the password method, and are reluctant to use or try any other login option.

There are significant differences in authentication preference by age group. For our analysis, we compared age broadly: those aged under 65 years with those aged 65 years and older. From this data, we see that those aged under 65 overwhelmingly prefer password authentication (mean rank = 1.29) over pattern and voice, while for those in the 65-and-older demographic, preferences are far more mixed. In the 65+ group we see a slight preference for password authentication (mean rank = 1.91), but not a strong preference, since the lowest ranked option, pattern, is only slightly behind (mean rank = 2.09). On the face, it makes sense that younger patients would prefer password authentication, the method with which they are most familiar. Younger people are likely used to remembering passwords for a variety of systems (or, more likely, reusing passwords between systems). Adding another system and another password to remember, while potentially burdensome, fits with these patients' expectations of what authentication looks like. Older patients may have poor eyesight, difficulty using a keyboard, have a hard time remember their password or do not have as much experience with password authentication, and thus would prefer a system using a method that has higher physical usability and rely less on cognitive memory.

Second, we see differences in ranking between PHR users and non-users. As shown in Table 2, the order of preferences between password, pattern, and voice (in that order) remains the same between the two groups, but for users of the PHR the preference is slightly stronger for passwords. Interestingly,

there was no correlation between age and PHR use, with the same percentage of people in each age group reporting that they were currently using the PHR (50%). Like the finding with age, we see again that it is likely that experience with a PHR, or experience with computer applications in general, seems to push the users' preference toward password authentication, the more familiar option. This finding makes sense when considering that a big issue with passwords is people's ability to remember them. More infrequent use, or non-use, correlates with a desire to use an authentication method that does not require remembering a nonsensical string of letters and numbers.

Some of the patients who were not frequent keyboard users and were not used to typing on the keyboard were happy to learn about the pattern login and voice login method. They commented that typing letters/digits, especially on a mobile device is difficult. Some mentioned they preferred pattern recognition and voice login over passwords especially on a smartphone or tablet. A few of the patients commented that they thought the voice login would affect their privacy if they tried to login using voice in public areas and therefore preferred the other login methods.

One of the patients who preferred the password login method commented that he thought the password was the most secure login method as it was more complex compared to pattern recognition or voice recognition method. He thought it was easier to hack a pattern login compared to the text password. However, when he was asked if he could remember and keep track of the passwords for logging in, he said that he usually writes down all his passwords in a book and stores them in front of his computer and therefore there is no need to remember the passwords. The patient did not consider writing down passwords could possibly compromise security.

Together, these results suggest that younger patients and more frequent users prefer to use the most commonly used authentication method: passwords. Less frequent PHR users and older patients have different and more varied preferences for authentication. It was outside the scope of this research to consider the relative security of the various authentication options. Users frequently use short passwords, easy to guess passwords, and passwords that are reused between several different sites. Each of these issues reduces the security of password authentication. Future research should investigate how people feel about the various authentication options if they are forced to choose unique passwords or patterns for each site, a recommended security practice.

In general, patients indicated strong security preferences for both their financial and health data. Our data show that patients care more about the security of their financial data than they do about their health data. This is likely due to the perceived level of risk associated with unauthorized access. While there are privacy implications to unauthorized medical record access, there are much more obvious and immediate consequences if someone gains illicit access to a financial institution account. This would be expected to vary depending on the context of the healthcare. Our study was conducted with cardiology patients, for whom there is likely little stigma. Patients receiving care for other conditions such as sexually transmitted diseases may have a different view on the privacy of their healthcare information.

CONCLUSIONS

In our study we found a statistically significant interaction effect between the ranking of authentication types and age. Further, a post hoc analysis of mean rank indicates that younger patients prefer passwords by a significant margin. Older patients indicated more mixed preferences.

Patients indicated a desire for security of their health information, though not as strong as their requirements for financial data. This could have significant implications on PHR designs and simplification of HIPAA laws, i.e. two-factor authentication for financial data but simpler authentication for health data.

While this study included a diverse group of patients and achieved significant results, the sample size was small and was intended as a proof of concept. It was also conducted with only patients in a cardiology clinic. More research to confirm and expand this research is necessary. Future studies should consider formal usability evaluations to compare patient authentication and security preferences.

This study has several contributions. First, it suggests that while passwords are the most popular, other authentication methods could be made available to patients to meet their needs and desires. Second, addressing the authentication usability barrier to PHR use by further understanding older patients' authentication preferences may help tip the scale to increased PHR adoption and regular usage. Third, to our knowledge this one of the first studies that evaluates *patients'* PHR authentication preference. We know that studying the usability from a user (e.g. patient) centered design approach is key to adoption and regular usage of PHRs by patients.

ACKNOWLEDGEMENTS

This project was supported by grant number HS022110-01A10 from the Agency for Healthcare Research and Quality. The content is solely the responsibility of the authors and does not necessarily represent the official views of the Agency for Healthcare Research and Quality. The authors would like to express their gratitude to the patients in the study. The authors would like to thank Aditya Chouhan a MIS graduate student for technical assistance in creating the prototype.

REFERENCES

[1] Administration on Aging. A profile of older Americans. 2002.
[2] Agresti A. 2002. Categorical Data Analysis. Hoboken, NJ: Wiley.
[3] Allaert FA, Le Teuff G, Quantin C, Barber B. 2004. The legal acknowledgement of the electronic signature: a key for a secure direct access of patients to their computerised medical record. International Journal of Medical Informatics;73(3):239-42.
[4] American Heart Association Statistics Committee and Stroke Statistics Subcommittee. Heart disease and stroke statistics 2017 at-a-glance.
[5] Android unlock pattern security analysis. 2012. [updated May 21]. Available from: https://sinustrom.info/2012/05/21/android-unlock-pattern-security-analysis/ . Archived at: http://www.webcitation.org/6uerL1mOR.
[6] Becker S. 2004. A study of web usability for older adults seeking online health resources. ACM Transactions on Computer-Human Interaction (TOCHI). Dec 1,;11(4):387-406.

[7] Berry N. 2012. PIN Analysis. Available from: http://www.datagenetics.com/blog/september32012/
[8] Blackwell DL, Villarroael MA. 2015. Summary Health Statistics: National Health Interview Survey, 2015.
[9] Bonneau J. 2012. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. 2012 IEEE Symposium on Security and Privacy, San Francisco, California.
[10] Brooke J. SUS-A quick and dirty usability scale. In: Jordan PW, Thomas B, Weerdmeester BA, McClelland IL, editors. Usability Evaluation in Industry. London: Taylor & Francis, Ltd; 1996. pp. 189-94.
[11] Chandra A, Calderon T. 2005. Challenges and Constraints to the Diffusion of Biometrics in Information Systems. Communications of the ACM. Dec;48(12):101-6.
[12] Chrischilles EA, Hourcade JP, Doucette W, Eichmann D, Gryzlak B, Lorentzen R, et al. Personal health records: a randomized trial of effects on elder medication safety. Journal of the American Medical Informatics Association. 2014 Jul;21(4):679-86.
[13] Clarke MA, Sitorius M, Windle T, Fruhling AL, Bernard TL, Windle JR. 2016A qualitative study of user-desired personal health record functionality: impact of age on desired PHR functionality. Abstract presented at the 40th American Medical Informatics Association (AMIA) Annual Symposium, Nov, 2016, Chicago, IL.
[14] Furnell SM, Dowland PS, Illingworth HM, Reynolds PL. 2000. Authentication and Supervision: A Survey of User Attitudes. Computers & Security. 2000;19(6):529-39.
[15] Furnell SM, Papadopoulos I, Dowland P. 2004. A long-term trial of alternative user authentication technologies. Information Management & Computer Security. 2004;12(2):178-90.
[16] Garfinkel SL. Email-based identification and authentication: an alternative to PKI? IEEE Security and Privacy. 2003;1(6):20-26. DOI: 10.1109/MSECP.2003.1253564.
[17] Health Information Technology for Economic and Clinical Health Act. 2009. HHS.gov
[18] Health Insurance Portability and Accountability Act of 1996, (Aug 21, 1996). HHS.gov
[19] How to attain meaningful use. [Internet].; 2013. Available from: https://www.healthit.gov/providers-professionals/how-attain-meaningful-use . Archived at: http://www.webcitation.org/6tST2tjYh.
[20] Irakleous I, Furnell SM, Dowland PS, Papadaki M. An experimental comparison of secret-based user authentication technologies. Information Management & Computer Security. 2002;10(3):100-108.
[21] International Organization Standardization (ISO). Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) - Part 11: Guidance on Usability. 1998 Jun 15,:22.
[22] Jones LA, Ant 'on AI, Earp JB. Towards Understanding User Perceptions of Authentication Technologies. Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society; Alexandria, Virginia, USA. New York, NY, USA: ACM; 2007.
[23] Kahate A. Cryptography and network security. Tata McGraw-Hill Education; 2013.
[24] Krist AH, Woolf SH, Rothemich SF, Johnson RE, Peele JE, Cunningham TD, et al. Interactive preventive health record to enhance delivery of recommended care: a randomized trial. Annals of Family Medicine. 2012 Jul;10(4):312-319.
[25] Kruse CS, Bolton K, Freriks G. The effect of patient portals on quality outcomes and its implications to meaningful use: a systematic review. Journal of medical Internet research. 2015;17(2):e44.
[26] Lowe G. A hierarchy of authentication specifications. Computer Security Foundations Workshop Proceedings. IEEE Xplore. 1997. DOI 10.1109.CSFW.1997.596782.
[27] McCallister E, Grance T, Scarfone KA. Guide to protecting the confidentiality of personally identifiable information (PII). 2010. NIST. SP 800-122.
[28] Price M, Bellwood P, Kitson N, Davies I, Weber J, Lau F. Conditions potentially sensitive to a personal health record (PHR) intervention, a systematic review. BMC Medical Informatics and Decision Making. 2015;15(1):32.
[29] Ricciardi L, Mostashari F, Murphy J, Daniel JG, Siminerio EP. A national action plan to support consumer engagement via e-health. Health Affairs (Project Hope). 2013 Feb;32(2):376-384.
[30] Selecting good passwords. 2017. [Internet]. [updated N.d.;]. Available from: https://csguide.cs.princeton.edu/accounts/passwords. Archived at: http://www.webcitation.org/6uerRKFmV. Princeton University.
[31] Selecting secure passwords. 2017. [Internet]. [updated N.d.;]. Available from: https://msdn.microsoft.com/en-us/library/cc875839.aspx . Archived at: http://www.webcitation.org/6uerbOzWn. Microsoft.
[32] Shah MH, Peikari HR, Yasin NM. The determinants of individuals' perceived e-security: Evidence from Malaysia. Int J Inf Manage. 2014;34(1):48.
[33] Toscos T, Daley C, Heral L, Doshi R, Chen Y, Eckert GJ, et al. 2016. Impact of electronic personal health record use on engagement and intermediate health outcomes among cardiac patients: a quasi-experimental study. Journal of the American Medical InformaticsAssociation. Jan;23(1):119-28.
[34] Undem T. 2010. Consumers and health information technology: a national survey. Lake Research Partners. Oakland, CA:.
[35] Weir CS, Douglas G, Richardson T, Jack M. Usable security: User preferences for authentication methods in eBanking and the effects of experience. Interact Comput. 2010;22(3):153-164.
[36] Zviran M, Erlich Z. 2006. Identification and Authentication: Technology and Implementation Issues. Communications of the Association for Information Systems. 2006;17(4):90-105.