2016

University of North Carolina Wilmington

Master of Science in

Computer Science and Information Systems

Proceedings

https://csbapp.uncw.edu/mscsis

A COMPARISON OF SECURITY AND PRIVACY PERCEPTIONS BETWEEN ROUTINE ONLINE ACTIVITY AND PERSONAL HEALTH RECORDS

Andrew Kuebler

A Thesis Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
of the Requirements for the Degree of
Master of Science

Department of Computer Science
Department of Information Systems and Operations Management

University of North Carolina Wilmington

2016

Approved by

Advisory Committee

Ulku Clark	Judith Gebauer
Devon Simmonds	Jeffrey Cummings Chair

Accepted By

_____
Dean, Graduate School

TABLE OF CONTENTS

Page

Abstract iii

List of Tables iv

List of Figures v

Chapter 1: Introduction 1

Chapter 2: Review of Literature Review and Analysis 4
- General Information Security 4
- Online Banking Portals 9
- Electronic Health Records 12
- Research Question: User Security and Privacy Perceptions of PHRs 14
- Model Development and Hypotheses 18
- Trust 20

Chapter 3: Methodology 22
- Population & Sampling Procedures 22
- Research Instruments 23
- Pilot Study 23

Chapter 4: Outline of Completed Thesis 26
- Data Collection 26
- Analysis and Results 27
- Physician Trust 32
- Qualitative Analysis 33
- Discussion 34

Chapter 5: Conclusions and Future Work 40
- Conclusions 40
- Future Work 40

References 42

Appendixes
- A. Pilot Study Results 45
- B. Final Survey (with changes from pilot study) 50

ABSTRACT

A Comparison of Security and Privacy Perceptions between Routine Online Activity and Personal Health Records.

Kuebler, Andrew, 2016. Capstone Paper, University of North Carolina Wilmington.

In today's connected world, everything is being done online. From paying bills to shopping to streaming music, most major services can now be handled without ever leaving your home. One major industry that has taken advantage of the Internet is the banking industry, where they have leveraged the Internet to allow consumers to handle their own banking transactions and services. Another industry that is just starting to utilize the Internet is the healthcare industry, where they are allowing patients to access certain sets of their health information through a Personal Health Record (PHR). Through a PHR, patients can communicate with their provider, request prescription refills, and view test results. With cyber-attacks occurring often in our connected society today, security and privacy are top concerns among all industries that allow people to access information online. This thesis researches how people perceive the security and privacy of an online banking portal compared to a personal health record, as well as what factors are driving these perceptions. Overall, there were no major differences in security and privacy perceptions between online banking portals and PHRs. Leading factors driving perceptions were website signals and brand reputation. However, it was found that patients are more likely to use a PHR if they have a trusting relationship with their physician. In terms of design enhancements, users would like to see better authentication controls, user alerts, and more visible security and privacy policies embedded in to PHRs and other online portals.

LIST OF TABLES

Table		Page
1.	Population Demographics	26
2.	SPSS Mean Comparison Results	29
3.	SPSS Mean Comparison Results – PHR Adopters	31
4.	SPSS Mean Comparison Results – Non-PHR Adopters	31
5.	Regression Analysis of PHR Adopters and Non-PHR Adopters	33

LIST OF FIGURES

Figure		Page
1.	Concerned Individuals on Privacy and Security of Medical Record	13
2.	Preferences of Sharing Health Information amongst Different Providers	14
3.	Methodology Model	18
4.	Map of Respondents	27
5.	Banking vs. PHRs: Security Variables Comparison	28
6.	Banking vs. PHRs: Privacy Variables Comparison	28

CHAPTER 1: INTRODUCTION

In today's world, it is evident that technology is a part of almost every industry in the United States. From manufacturing to online retailers to various service industries – it seems that most companies are leveraging technology for their benefit. However, one industry that is seriously lacking is the healthcare industry. Currently, hospital networks across the United States are in the process of implementing electronic health record systems, which is revolutionizing the way doctors practice medicine because these systems eliminate many manual processes, one of which is paper charting. In 2009, current President Barack Obama called for healthcare networks across the country to implement electronic health record systems within five years (Childs et al., 2009). Under this federal mandate, Obama envisioned that these systems would improve patient care and ultimately lower the cost of medical treatment (Childs et al., 2009).

Today, many hospital networks have implemented various electronic health record systems across the country with the hope of simplifying patient care. Formally defined, an electronic health record (EHR) contains digital records of health information which can include past medical history, vitals, progress notes, diagnoses, and various reports (Weiss, 2015). However, the real power behind an EHR is how the data is shared – as they can be shared across private practices and various health networks – allowing for an easy and convenient coordination of care among all of the clinicians involved with that particular patient regardless of location (Weiss, 2015). Another commonly used term, electronic medical record (EMR), is basically a digital version of a paper chart (Weiss, 2015). They contain a lot of the same information that an EHR does, but they lack the ease of sharing between practices and health networks, unlike an EHR (Weiss, 2015). While the terms EMR and EHR have been used interchangeably, more and

more people are referring to the technology as an electronic health record (or EHR) (Weiss, 2015).

Along with these electronic health record systems, many vendors have the option of implementing another variation of an electronic health record, known as a personal health record (PHR), which provides patients limited access to their own health record through an online web portal (they do require a username and password), and contains some functionality such as requesting prescription refills and contacting their primary care provider. These records contain a lot of the same information as an electronic health record. It is also important to note that while an electronic health record has its data populated by only medical staff, a personal health record can be populated by the medical staff or the patient directly. In other words, though they are distinct data sets, an electronic health record is used *internally* – between doctors and medical staff and hospital networks – while a personal health record is used *externally* and is managed by the patient.

With cyber-attacks and security breaches becoming more prominent, people are concerned about the security and privacy of their information. And now with health information available online, a new target exists to gather personal information for identity theft purposes. However, people have been using online portals for banking, shopping, and other various transactions for years now. This research seeks to learn how people perceive the security and privacy of the newest type of online portal – the personal health record. To understand user perceptions of PHR portals, the study compares PHRs to everyday online activity, specifically online banking portals. To accomplish this, a quantitative, statistical analysis of survey results is conducted. Furthermore, a qualitative analysis of user concerns over privacy and security is conducted in order to make portal design recommendations based on current concerns.

In order to gather a large amount of data to determine how the general public perceives the security and privacy of personal health records, a survey was used. This survey is filled with various questions around security, privacy, and trust. In addition, the participants are shown screenshots of a banking portal and a personal health record that they can assess when making their determinations as to how secure and private they feel their information is in these portals. From the data gathered, an analysis was conducted in order to understand how the participants perceived the security and privacy of personal health records. Based on privacy and security concerns, the final outcome of this research was to combine these concerns with their perceptions and make a set of recommendations to electronic health record vendors that they can use in future software releases in order to help eliminate any security and privacy concerns barriers.

The thesis is structured as follows: Chapter 2 covers the literature review and related work, Chapter 3 explains the methodology in more detail, Chapter 4 discusses the results and analysis, and Chapter 5 concludes the research and introduces potential future work.

CHAPTER 2: REVIEW OF LITERATURE REVIEW AND ANALYSIS

The literature review consists of three specific areas concerning user security and privacy perceptions including general information security, online banking portals, and electronic health records (EHRs). In addition, a more focused literature review was done around personal health records, however there is limited research in this area as it is an emerging field of security studies. There is an abundance of literature on user security and privacy perceptions as it pertains to general information security when compared to perceptions of electronic health records. With respect to each area, each had their own trends. In terms of general information security perceptions, the consensus was that users want their technology to be secure, however they also value the technology's usability and convenience (Abdulwahid et al., 2015; Weir et al., 2009; Kim et al., 2010). Another strong correlation from the research was that users, both business and consumer level, are not taking information security precautions and behavior seriously, unless mandatory (Boss et al., 2009; Teer et al., 2007). For perceptions of online banking portal adoption, the results were mixed. Some studies found security and privacy perceptions played a more crucial role in determining whether people used online banking portals, while some studies did not find this correlation. Finally, for perceptions of electronic health records, the consensus was that users are generally concerned about the security and privacy of electronic health records. In the subsequent sections, a detailed review of each area is presented.

General Information Security

Information security has always been something that both users and companies struggle to deal with, both internally and externally. Prior research ranges from focusing on getting security and privacy perceptions of certain technologies to the practices that home users and businesses use (Boss et al., 2009; Anderson & Agarwal, 2010; Teer et al., 2007). One particular

study set out to develop the model of the "conscientious cybersecurity citizen (Anderson & Agarwal, 2010)." The study proposed that the "conscientious cybersecurity citizen" is someone that "believes taking information security precautions is a desirable action," and "has concerns around security threats, perceived citizen effectiveness, and self-efficacy (Anderson & Agarwal, 2010)." The results reinforced their proposed model that a "user's attitude toward security-related behavior is influenced by concern regarding security threats, perceived citizen effectiveness, and self-efficacy (Anderson & Agarwal, 2010)." In addition, it was found that users must believe in the precautions, and the more positive the attitude, the more likely the user will make an effort to protect themselves (Anderson & Agarwal, 2010).

Another study looked at undergraduate university students in computer information systems, art, and integrated science and technology programs to determine the security controls they use and how they perceived the importance of computer security (Teer et al., 2007). The results showed that 60% of students felt that their personal computers were somewhat insecure (Teer et al., 2007). In terms of their personal security perceptions, 46% responded that security was very important to them personally, but yet another 40% responded that security was somewhat unimportant to them (Teer et al., 2007). The only consensus that was reached was when the students were asked about the importance of security as it pertains to businesses. In an almost unanimous vote, 96% of students thought that security was very important for businesses (Teer et al., 2007). Furthermore, these students felt security applies more to corporate settings than to them personally.

Other studies have focused on the use of security in the business environment. For example, one study used a model to explain how end users approach information security in a business setting, using the idea of "mandatoriness (Teer et al., 2007)." The study defined

"mandatoriness" as "the degree to which individuals perceive that compliance with existing security policies and procedures is compulsory or expected by organizational management (Teer et al., 2007)." In this study, it was determined that if the policy was perceived to be mandatory by users (with influence and pressure from upper management), then they took the information security precautions more seriously (Teer et al., 2007). Another study further examined security and privacy perceptions in the corporate setting by examining how directors and senior level managers view organizational information security (McFadzean et al., 2007). Interviews were conducted with those in executive-level and Board of Director positions (McFadzean et al., 2007). Researchers found that the higher the perceived risk of security, the greater need for a security control to mitigate the risk (McFadzean et al., 2007). Another interesting result to note that the perceptions depended on the participant. Some directors saw a security breach as low risk with minimal consequences, while others will constantly review security architecture and policies to bridges any gaps in their security defense (McFadzean et al., 2007).

Lastly, researchers in another study researched how the areas of organizational climate (how the organization deals with members), self-efficacy (an individual's belief in their ability to perform a specific task), management practices (perceived actions of managed observed by the employee), supervisory practices (observed and repeated actions of direct supervisors), and coworker socialization (daily interactions with coworkers) impacted employee perceptions of the organization's information security climate (Chan et al., 2005). The study concluded that the three areas of coworker socialization, direct supervisory practices, and upper management practices all had a positive relationship with an employee's information security perceptions within the organization (Chan et al., 2005). As a result, and outside the scope of this research,

these perceptions combined with self-efficacy influenced whether employees were compliant with information security behaviors (Chan et al., 2005).

In essence, in terms of both business users and the general public, individuals are not taking a proactive approach to information security behavior and precautions unless they are forced to implement such a mindset. However, those that positively view information security as well as those who trust security precautions are more likely to protect themselves when interacting with online portals. As the research has shown, some executives take information security more seriously than others, as some view security breaches as an event with little consequences while others are constantly reviewing policies to bridge any security gaps. This in turn flows down and affects the employee perceptions of information security, as their perceptions of how directors and upper management handle information security aids in determining how they themselves will perceive information security and whether or not they will comply with information security procedures and policies set by the organization.

Besides the consensus of users not taking the correct approach to information security, when it comes to specific technologies, users want something that is secure, but yet extremely simply to use as well (Abdulwahid et al., 2015; Weir et al., 2009; Kim et al., 2010). One study that reflects this conclusion was done on how people perceive e-banking tokens that are used for authentication (Weir et al., 2009). The participants were given a few different e-banking tokens to test, and the study looked at how the subjects perceived each token's usability, usage, quality, security, convenience, and security ratings (Weir et al., 2009). The results suggest that people chose the device that was easiest, which also happened to be the least secure (Weir et al., 2009). In another study, researchers examined the perceptions of current authentication techniques (Abdulwahid, 2015). It was found that users do not mind the idea of applying authentication

security, but like the previous study, they want to avoid the common hassles behind it (Abdulwahid, 2015). Another study researched undergraduate students in Spain as they used two web-based simulators to simulate securities transactions (e.g. trading stocks), and the students were given a survey to test their perceptions around trust, security, and privacy with the proposed research model (Carlos Roca et al., 2009). The goal of the study was to determine how electronic investors were influenced by perceptions around trust, security, and privacy (Carlos Roca et al., 2009). Based on their questionnaire, researchers found that trust, usefulness, and ease of use are the most important influences in using online trading systems (Carlos Roca et al., 2009). This further strengthens the conclusion that end users want systems that are easy to use, but effective and secure as well. In addition, if the students had high perceptions of security, then those determined a level of trust; however, if the students had lower perceptions of trust, then the security had to be improved in order to enhance trust (Carlos Roca et al., 2009).

In terms of privacy perceptions, high perceptions of privacy did not correlate as strongly to trust as security did (Carlos Roca et al., 2009). Lastly, a study examined consumers' perception of security and trust and how it affected their use of electronic payment systems (Kim et al., 2010). While implementing certain technical safeguards and security statements helped to increase user perceptions of security (which impacted how they used the electronic payment system as well), results showed if consumers experience any inconvenience in the system, then this may negatively impact their perceptions of the security and trustworthiness of the system, and it can cause system designers to go back to the drawing board to implement more convenient, usable systems (Weir et al., 2009).

Based on these studies, it is clear that users are easily frustrated with information security safeguards, and they want the most minimalistic and transparent, yet secure, tools so that they do

not hinder their daily lives and time. The current study investigates whether these perceptions are different for a PHR (versus a banking portal) as a personal health record contains more sensitive and unique information, such as medical history and allergies, which could be leveraged inappropriately if the wrong people were to get a hold of a person's electronic personal health record and the information it holds.

Online Banking Portals

Since it would be difficult to test user security and privacy perceptions of personal health records against every publicly accessible online technology available, this research specifically focuses on online banking portals as the more mature technology for comparison. There is an abundance of literature around what factors cause people to adopt or not adopt online banking. While some studies found security and privacy to be leading factors, others did not.

One of the first studies that examined online banking portals concluded that people just do not like the idea of giving out personally identifiable information or financial information over an electronic medium such as a website or telephone (Hoffman & Novak, 1998). This was not a surprising conclusion considering the ongoing advancement of technology in today's society. Another interesting perception that was found in one study was that the population thought the banks should be the ones concerned about security and privacy – that is it should be their responsibility to protect them from fraud and other illegal financial activities – and not a responsibility for the end user to handle (Jahangir & Begum, 2008). Researchers in another study looked at how security, privacy, usability, and reputation of a website influence consumer trust in online banking (Casalo et al., 2007). The results found that security, privacy, usability, and the bank's brand reputation all had a direct and significant effect on whether consumers trusted and utilized an online banking portal (Casalo et al., 2007). Researchers also concluded that given

security and privacy scored so high, it could be possible that security and privacy concerns could prevent the growth of e-commerce business operations in the future (Casalo et al., 2007). Another study that coincided was done in Australia, where researchers there also found that security and privacy were some of the leading factors in adoption and carrying out online banking transactions (Sathye, 1999).

While this research seems to conclude that security and privacy concerns influence adoption, there was other research that found other factors that influenced the adoption and use of online banking portals. Researchers in one study developed a model to determine how private banking customers accepted online banking in their home country of Finland (Pikkarainen et al., 2004). The factors that they tested were perceived usefulness; ease of use; enjoyment; information on online banking; security and privacy; and the quality of Internet connection (Pikkarainen et al., 2004). The results of their study found that site usefulness and whether or not they could find information on online banking on the site were the two largest factors that drove adoption (Pikkarainen et al., 2004). It is worth noting that security and privacy was not the highest scoring factor as other research has found. The researchers ran three different analyses: factor, regression, and correlation, in order to test their hypotheses. In the factor analysis, security and privacy had a score of 3.467, placing second to perceived ease of use with a 3.628 (Pikkarainen et al., 2004). In the regression analysis, security and privacy did appear to be the most significant factor with a significance rating of 0.933 (Pikkarainen et al., 2004).

Lastly for the correlation analysis, security and privacy did not have any positive correlation with consumer use (Pikkarainen et al., 2004). Factors that scored the highest in the correlation test were perceived usefulness and the amount of information available in the portal. Based on their overall results from their three analyses, the researchers did not find security and

privacy to be the most influential factor for the consumer adoption of online banking. Another study conducted in Bangladesh looked at two different models around online banking usefulness, security, and privacy (Jahangir & Begum, 2008). The researchers determined that their population viewed online banking to be secure as it scored a 4.4 out of a five-point scale, thus concluding that this population was not as concerned about security and privacy (Jahangir & Begum, 2008).

A study examining factors of adoption of e-banking technologies found that factors such as complexity, simplicity, compatibility, observability, risk tolerance, and product involvement all influenced the adoption of e-banking technologies (Kolodinsky et al., 2004). In addition, simple demographics can also be factors driving adoption including the user's income, education, gender, and marital status (Kolodinsky et al., 2004). Those with a higher income and education were more likely to adopt an online banking portal within the next year, while those that were sixty-five years of age or older were less likely to adopt an online banking portal within the next year (Kolodinsky et al., 2004).

With all of the research presented around online banking portals, it is clear that the research is volatile when it comes to how people perceive online banking portals and what factors drive adoption. While some studies found security and privacy to be leading factors in online banking adoption, others did not find those factors to be as prominent and favored usefulness, the information content of the portal, and common demographic factors instead.

As this study compares security and privacy perceptions of online banking portals with personal health records, we feel that the perceptions for personal health records would be more critical as health records contain much more sensitive information (e.g. allergies, immunizations,

lab results, etc.) in addition to information already found in banking portals such as credit cards and other billing information.

Electronic Health Records (EHRs)

In addition to security and privacy in the online banking discipline, researchers have begun to focus more narrowly at specific industries including the newly emerging area of electronic health records. However, since electronic health records are still an emerging technology with many still being implemented in hospital networks across the country, there are limited studies focusing on an individual's perceptions of EHRs. Of the research available, it is clear that users are concerned to some degree with the security and privacy of their information in an electronic health record (Patel et al., 2015). Based on a study from 2013, around 70% of those that were surveyed were "very or somewhat concerned" about the security and privacy of their medical record. In addition, as a result of these concerns, some participants (8%) were so unsettled that they even withheld some of their medical history or other pertinent information from their provider (see Figure 1) (Patel et al., 2015). Despite the general concern, other research shows that if adults felt they were receiving higher quality care, then they were not as concerned with privacy and security and withheld less information from their provider (Patel et al., 2015; Campos-Castillo & Anthony, 2015). Another study found that 48% of their participants were "very concerned" about the privacy of the health record (Carlos Roca et al., 2009).

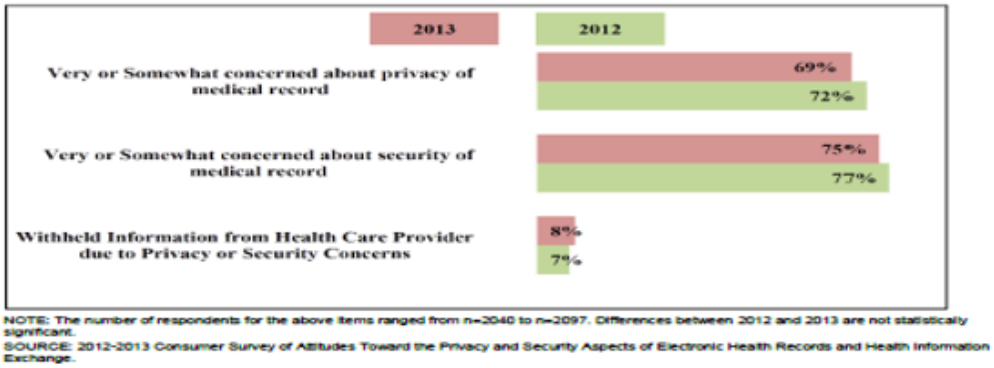


Figure 1: Concerned Individuals on Privacy and Security of Medical Record (Patel et al., 2015)

Since security and privacy are a large concern among the public, one study looked at how people would share their information with a variety of providers, if given the opportunity (Caine & Hanania, 2013). The study ultimately found that people are not looking to share all their information with everyone unconditionally, rather they want to share certain types of information (e.g. the more sensitive information) with certain groups versus the less sensitive information (Caine & Hanania, 2013). Figure 2 reflects this information. In a similar study, participants wanted to be able to control who could access what information and wanted to be notified when their data was accessed (Caine et al., 2013). It can be concluded from the research presented that security and privacy concerns are prominent among the general public; however, what the research is lacking is why specifically people are concerned about the security and privacy of electronic health records.

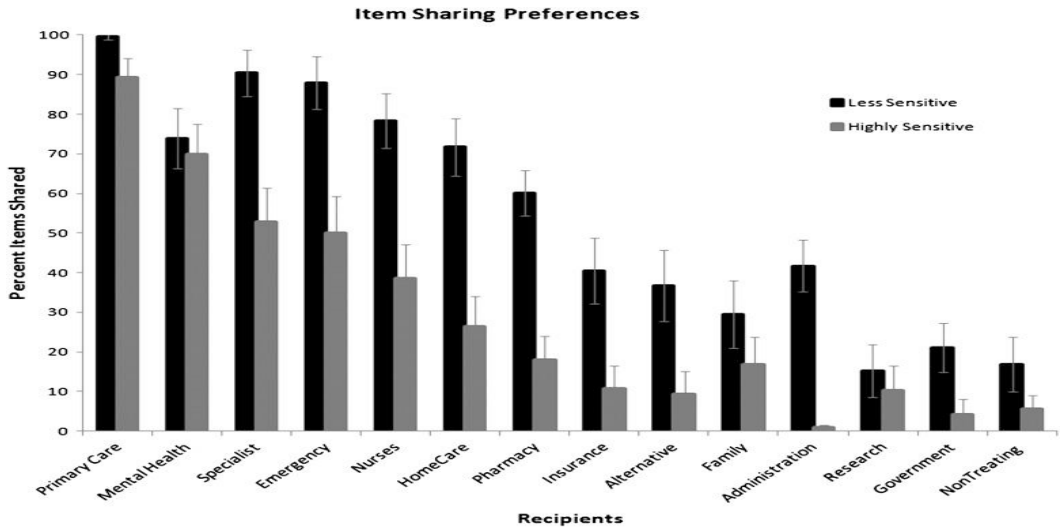


Figure 2: Preferences of Sharing Health Information amongst Different Providers (Caine & Hanania, 2013)

Despite the general concerns presented, people had an interesting as well as a contrasting perception as to whether or not electronic health records should be used. With these privacy and security concerns in mind, people still felt that electronic health records should be used (Patel et al., 2015; Gaylin et al., 2011). One study found that even though their participants were concerned, 64% of them agreed or strongly agreed that the benefits of using electronic health records exceeded any potential privacy risks (Gaylin et al., 2011). Another study concluded that despite security and privacy concerns, 76% of participants still wanted their health care providers to use an electronic health record (Patel et al., 2015).

User Security and Privacy Perceptions of Personal Health Records (PHRs)

As shown above, a majority of the research shows the security and privacy concerns of people as it pertains to the *internal* use of their electronic health record (e.g. amongst other providers and during clinical office visits). However, there is now a newer, more personal way of viewing your health information, and it is through the use of a personal health record. This is a contrasting approach to previous research as personal health records are *external* and can be accessed via anyone with a web browser. Since this is still a newer technology to hospitals and

patients, and is usually implemented after the electronic health record is running and stable, the research in this domain is limited.

Currently, research has focused on patient use and general feelings about the idea of a PHR. Preliminary research shows very few people, as little as 20%, are currently using a PHR (Dimitropoulos et al., 2011). The same study found that almost 80% of people believed that a PHR would be a good informant of health information for patients, and the research also showed that only 60% of people thought it would help reduce medical costs (Dimitropoulos et al., 2011). Another similar study looked at the consumer attitudes of PHRs and how many of people used the Internet for looking at their PHR (Wen et al., 2010). The results showed that 86% of participants felt that access to their PHR was important, with approximately 47% of those people saying it was very important (Wen et al., 2010). However, despite the importance, only 9% of people used the Internet for checking their PHR; younger people valued the PHR more than older participants, and those with a health care provider were twice as likely to use the Internet for checking their PHR (Wen et al., 2010). In terms of perceptions, privacy and security perceptions are positively correlated with the perceived value of the PHR (Emani et al., 2012). This study cited that as long as providers are willing to encourage patients to use this new technology, then patients will be more likely to adopt this technology for themselves (Emani et al., 2012). These studies clearly demonstrate that there is a gap between their perceptions and actual usage, as many people think it is important, but yet few users access PHRs.

Other studies have approached the perceptions of PHR from the point of view of physicians and their support staff. Medical staff view a PHR as an alternative source of a patient's medical information for the health care provider when their complete and actual electronic health record was not available (Witry et al., 2010). Staff members feel PHRs could

help increase efficiency within a hospital or physician practice (Witry et al., 2010). However, even medical staff are often unaware of what PHRs can do. Providers were often unaware of the features of a PHR that a patient could utilize, and they ultimately thought patients would not take the time to create one and update it on a regular basis (Witry et al., 2010). Additionally, providers specifically pointed out the prescription refill feature – saying that PHRs could actually promote drug abuse (Witry et al., 2010). Thus, there seems to be differing opinions of the benefits of PHRs among patients and medical staff. Patients seem to view PHRs as a more useful, beneficial tool, while providers seem to have more critical perceptions and only intend to use them if other sources of a patient's medical information are not available. These critical physician perceptions could also be one of the factors that is hindering the widespread adoption of personal health records.

From the research presented above, it can be concluded that there is an abundance of research for the areas of user perceptions of general information security, online banking portals, and electronic health records. In terms of general information security, people want technology that is secure, but they are willing to make the tradeoff for something that is more convenient for them. In addition, users do not take their own personal security seriously, and they feel it applies more to the corporate settings. For security and privacy perceptions of online banking portals, some studies found that security and privacy perceptions influenced adoption, while others did not and one study even found demographic information to have an influence on adoption. For user security and privacy perceptions of electronic health records, the majority of people are somewhat concerned with how their information is used internally amongst providers and during clinical office visits. Lastly, personal health records are on the rise, and the preliminary research shows a positive correlation between security and privacy perceptions and the value of a PHR.

While patients are more open to the usage of personal health records, providers and medical staff view them as more of an internal tool, and they have their reservations when it comes to some of their features and whether or not patients would actually create them and keep up with them.

As mentioned, the research in this area is evolving, and the intent of the current thesis is to take a closer examination of PHR use. While research has looked at general perceptions, this study is more concerned with security and privacy perceptions. An additional topic of interest will be how factors of trust influence these security and privacy perceptions. The goal of the current study is to help add some different points of view and richness to the research area of the perceptions of personal health records. Based on the research presented, this thesis seeks to expand on the research of perceptions of personal health records by diving in to the security and privacy perceptions of personal health records and comparing these perceptions to the security and privacy perceptions of routine online usage – such as using an online banking portal. Specifically, the research seeks to answer the following questions:

1. Are there differences between user security and privacy perceptions of everyday online activity – such as using a banking portal or shopping online – and user security and privacy perceptions of a newer, external method of accessing your health information, the personal health record?
2. Does the factor of trust have any influence on the security and privacy perceptions of personal health records and routine online activities?
3. If there are concerns of security and privacy with personal health records, then what are the explicit reasons for concern?
4. With these concerns in mind, can recommendations and conclusions be given to vendors to aid them in breaking down this barrier for future releases?

Model Development and Hypotheses

The goal of this research is to determine if user security and privacy perceptions of routine online activity differ from personal health records. Since it would be difficult to look at all routine online activities, the research uses online banking through internet portals as the routine online activity. The research also examines how trust affects these perceptions. Based on the results, a detailed analysis of explicit concerns surrounding personal health records is performed and from these concerns, recommendations are drawn in order to help positively change perceptions in future PHR releases. In order to answer the research questions posed, the following model (Figure 3) will be applied from a prior study on security perceptions and trust (Ray et al., 2011). This model is adapted to fit this study on the comparison between routine online activity and personal health records.

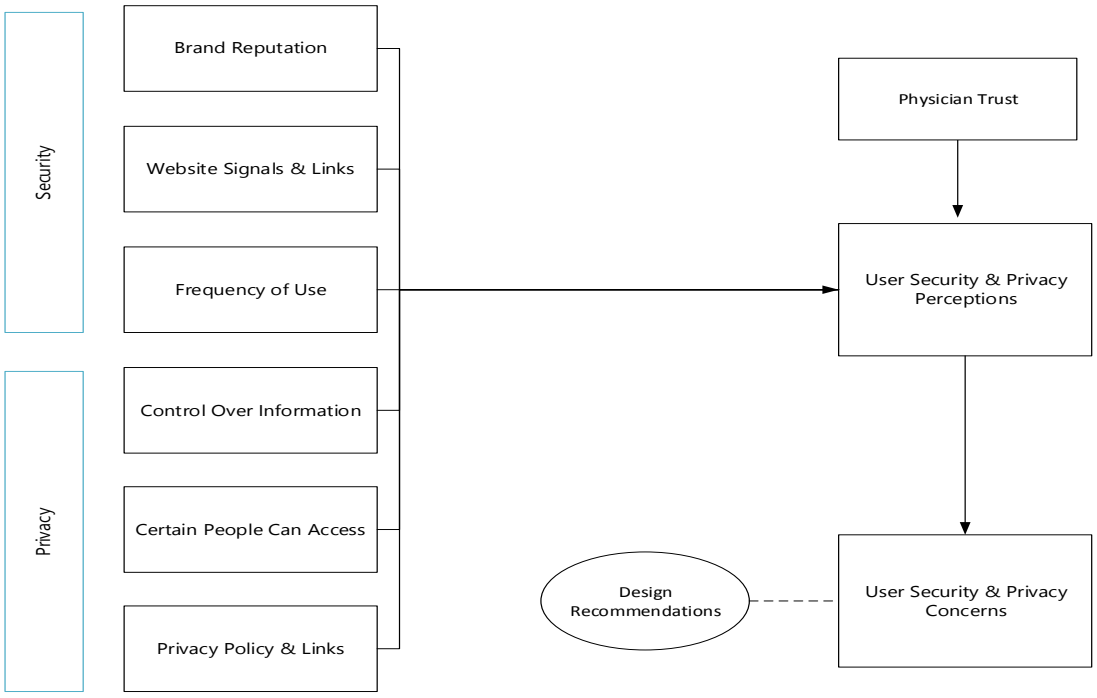


Figure 3: Methodology Model (adapted from Ray et al., 2011)

In order to gain perceptions around security, this research examines three different areas that influence user perceptions of security: (1) overall brand or domain name reputation, (2)

website signals (e.g. the lock button specifying https on the website), and (3) site utilizations (i.e. frequency of use). In order to determine how users perceive privacy amongst the two portals, this research examines: (1) the degree to which users feel they have control over their information, (2) the degree to which users feel only certain individuals can access their information, and (3) the understanding of clearly stated privacy policies.

The current research proposes that the above factors will be viewed differently when accessing a banking portal compared to a personal health record portal. With personal health records and their relative "newness", users may be skeptical about this technology that houses sensitive, personal information. Physician apprehension in the technology may also compound the problem. Physician and other medical staff hesitation over the use of personal health records may increase a patient's hesitation of accessing this information through online portals. Contrary to PHR portals, users have been interacting with banking portals extensively over the past 10 years and the technology itself has become well-established. Because of this, users may have reduced privacy and security concerns with a mature technology such as banking portals. Based on these factors, a user will have increased security and privacy perceptions of accessing personal health records compared to online banking portals. Thus,

Hypothesis 1: Users of personal health record portals will have greater concerns across the factors of security and privacy compared to online banking portals.

While these factors may be significantly different between the two portals, it does not mean that all factors are equivalent when it comes to privacy and security concerns. Specific factors may be more significant on security and privacy perceptions when compared with others. For security, the "Website Signals and Links" factor may be more influential than others as this is simple cue that is easily understood by many users as suggesting security. This includes simple elements such as the "https" in the web address or the green lock symbol that appears next to the

URL that the population are most likely to associate with security and are familiar with from every day online activity. Therefore,

Hypothesis 2: Website Signals will have the highest influence on security perceptions compared to the other factors.

Prior research suggests that users are often concerned for who can actually view their patient information in EHR systems (Caine & Hanania, 2013). This suggests the factor concerned with who can access this information may be more significant than other privacy factors. Individuals only want to share certain sets of their information with certain types of people and they do not want any one person to see all of their information. Thus, this factor will be greater compared to other privacy concerns within PHR portals.

Hypothesis 3: Individuals who have access to a patient's data will have the highest influence on privacy perceptions compared to the other factors.

Trust

The research up to this point explains what has been conducted in the areas of security and privacy perceptions of general information security and personal health records. While the main point of this research is to look at security and privacy perceptions, another domain that the research examines a user's trust in online environments. Trust can be examined from various perspectives including an individual's disposition to trust and physician trust.

Disposition to trust is commonly used to measure an individual's willingness to trust other individuals or online environments. This measures the individual's inherent disposition to trust others. More recently, researchers have begun to examine the impact physician trust may have across a number of factors. Factors influencing physician trust include length of relationship, ability to choose, physician involvement and expectations of quality care (Thom et al., 1999). This research has found that trust is positively correlated with participant satisfaction

(Thom et al., 1999). While this research primarily focuses on the face-to-face relationship among the patient and physician, physician trust may also impact how online PHR portals are perceived by users. If users have increased trust in their physician, this trust will translate to the online environment, increasing the perceptions of security and privacy within the PHR portal. Thus,

Hypothesis 4: Increased trust in a user's physician will reduce concerns of security and privacy in online PHR portals.

Each of these hypotheses were tested using the methodology model in Figure 3. The results from these hypotheses can be found in the analysis and results section in Chapter 4.

CHAPTER 3: METHODOLOGY

A questionnaire was used in order to test the research model. The target population was adults over the age of 18 and focused on those who had the potential of using both online banking portals as well as PHR portals. To ensure the survey questions had face validity and were easily understandable by participants, a pilot study was conducted using undergraduate classes at the Junior/Senior level. While this was not the target demographic for the current study, the pilot test resulted in feedback from participants around the structure of the survey and aided in clarifying confusing or confounding questions found in the survey. The feedback was incorporated in to the final survey before being sent out to the final participants through email, social media, and Amazon Mechanical Turk. The completed surveys were then used to analyze the proposed model and make design recommendations based on the results concerning the factors that influence security and privacy concerns surrounding PHR portals.

Population

For this research, participants were taken from the general public in the United States. The questionnaire required that people be over the age of eighteen in order to participate. However, in order to get the most accurate results, the ideal target population was those with a medical history and possessed an ongoing relationship with their primary care physician, thus skewing the target population to those in the older demographic.

Sampling Procedures

Since it would be nearly impossible to gather perceptions on every individual that meets the requirements of the target population, a random sample was taken by using an online survey response tool. The survey was posted for a limited amount of time, and those that are able to respond to the questionnaire within the time frame will be a part of the survey results.

Research Instruments

Due to the scope of the research and the population to be sampled, a questionnaire was the simplest and most effective way to gather an abundance of responses. The survey was created using the Qualtrics platform, and it was distributed to potential participants electronically through Amazon Mechanical Turk, a service of Amazon Web Services. Amazon Mechanical Turk is a survey administration tool that allows researchers to publish surveys in order to quickly gather responses in exchange for a small fee that is made to each participant for taking the time to complete the survey.

The questionnaire developed was structured around two main disciplines: online banking portals and personal health records. The questionnaire first asked questions around the participant's frequency of Internet use in addition to how they evaluate their personal trustworthiness before being presented with questions around the online banking portal and PHRs. After gathering the participant's Internet use, the participant was asked questions around online behavior and PHRs, with questions pertaining to each of the six respective factors in the model. The last section of the survey gathered various demographics about the participant for additional analysis. The entire questionnaire can be found in Appendix B of this research.

Pilot Study

A pilot study with the survey was conducted in late October 2015. The purpose of the pilot study was to ensure the questions were in a readable and understandable format before sending it out the general public through Amazon Mechanical Turk. For the pilot study, two classes of undergraduate information systems courses were used. In total, there were 55 participants, and it was found that the majority of them spent about 5-7 hours online a day (see Table A1 of the appendix). However, despite all of this time online, very few of them used the

Internet to access their PHR (69% of the participants never or rarely accessed their PHR online). Besides basic Internet usage, the participants were also surveyed on their concerns of online banking portal and PHR security and privacy. In terms of online banking security, participants are most concerned about them requiring a strong username and password; for PHR security, participants are most concerned about the URL beginning with "https://." For online banking privacy, participants are most concerned about hiding sensitive information from an employee; for PHR privacy, participants are most concerned about only allowing authorized personnel to view their personal information. Complete pilot study results can be found in Appendix A.

Survey Changes

After each class completed the questionnaire, the students were debriefed and asked questions concerning their thoughts about the survey in terms of format and readability. Participants mainly pointed out wording and continuity issues. The main continuity issue was that since a lot of the questions applied to both online banking and PHRs, the term would show up in questions that were opposite to the domain we were testing (e.g. the phrase "online banking" would show up in the PHR questions). However, one issue that was voiced amongst several participants was that they were only able to view the respective screenshots one time. Participants requested for future use that the screenshot be available on multiple pages, or that they have the availability to go back and view the respective screenshot as needed. Another, but significantly more uncommon issue amongst the participants, was that the Qualtrics display logic feature may have been set up incorrectly, as a couple of participants would select an answer and get a follow up question due to how they responded to the previous question when it was not necessary. These changes were made before the final questionnaire was administered on Amazon

Mechanical Turk and to our participants not on Amazon Mechanical Turk. The complete and final questionnaire that was distributed to participants can be found in Appendix B.

CHAPTER 4: OUTLINE OF COMPLETED THESIS

The following sections include a description of the data collection, analysis, and findings.

Data Collection

Data collection began in the beginning of the spring semester. A Human Intelligence Task (HIT) was published on Amazon Mechanical Turk that requested participants interested in sharing their thoughts concerning online security and privacy. Participants accepting the HIT were instructed to follow a link to the Qualtrics survey and upon completion of the survey, they were given a verification code to collect their fee. This link was also made available to non-paid participants as well. The survey was distributed through social media websites including Facebook and LinkedIn. These participants were also directed to Qualtrics to take the survey, but there were no fees involved for their participation.

In total, there were 304 participants that took the survey. The demographics of the participants are included in Table 1 below:

Gender	%
Male	46
Female	54
Age Range	
18 – 24	13
25 – 34	43
35 – 44	20
45 - 54	11
55 +	13
Ethnicity	
African American	9
Asian	5
Caucasian	79
Hispanic	5
Other	2

Table 1: Population Demographics

The HIT was restricted to the United States to limit participants to a country in which both banking and health portals are available. Figure 4 below shows an aggregate mapping of where

our participants were located throughout the United States. As depicted in the graph, most of our participants came from the East Coast and the Midwest.

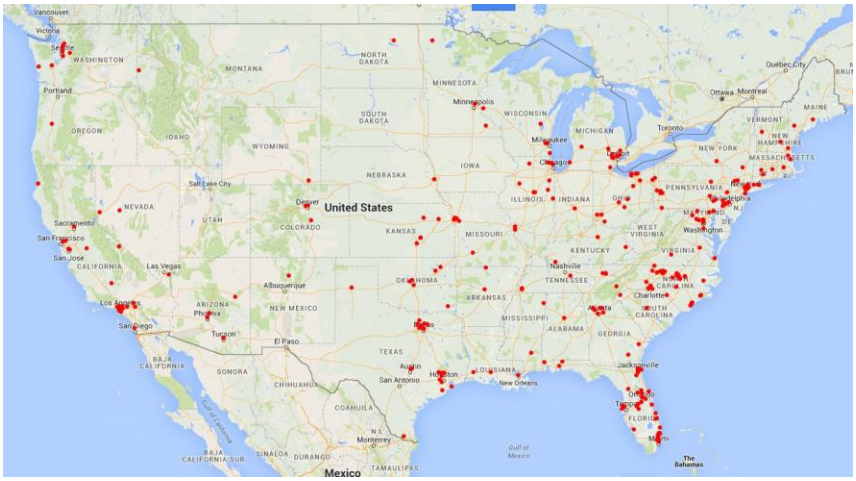


Figure 4: Map of Respondents

Analysis and Results

To test the hypotheses, a mean analysis was first conducted to examine the difference between online banking and PHR portals across the security and privacy factors. The security variables or factors compared were overall brand reputation, website signals, and frequency of use. The privacy variables or factors compared were having control over information, having control over who can access information, and the presence of privacy policies and links. The score for each variable was based on a score out of a five-point scale. Before analyzing the variables, the mean analysis looked at overall usage of the two technologies. Out of the three hundred and four participants, 68% had used an online banking portal while only 31% had used a personal health record.

When the mean analysis was conducted on the security variables, brand reputation scored a 3.88 for banking portals versus a 3.74 for PHRs. For website signals, the gap was even less with a 3.60 for banking portals and a 3.57 for PHRs. Lastly for frequency of use, banking portals scored a 3.11 and PHRs had a 2.90. The results can be summarized by Figure 5 below.

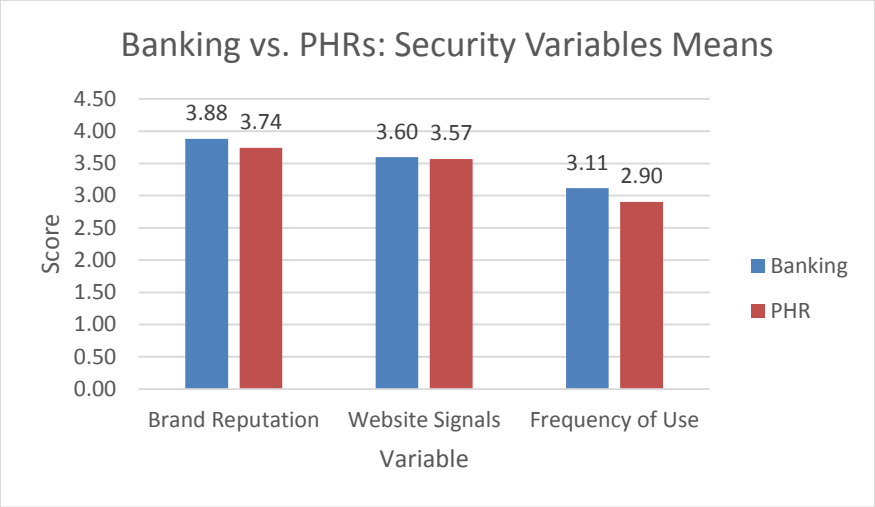


Figure 5: Banking vs. PHRs: Security Variables Comparison

For the privacy variables, having control over information resulted in a tie, with a score of 4.21 for both banking portals and PHRs. In terms of having control over who can access their information, banking portals scored a 4.40 versus PHRs with a 4.34. Lastly, for the privacy policies and links variable, banking portals scored a 3.86 while PHRs scored a 3.85. The complete results can be summarized by Figure 6 below.

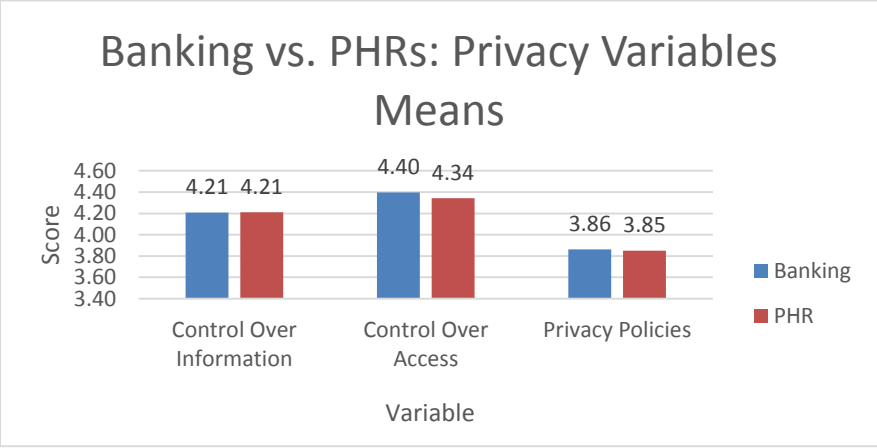


Figure 6: Banking vs. PHRs: Privacy Variables Mean Comparison

To further analyze the difference between the portals, a mean comparison was conducted using IBM's SPSS 22 statistical analysis software package. When importing the data in to SPSS, the data was immediately cleansed to get rid of outliers (e.g. people that selected all ones or fives in order to complete the survey more quickly). The following two questions (i.e. general privacy

and security concerns) were included in the mean comparison to understand the general concerns of respondents across both privacy and security:

1) How concerned are you about the security of your information in a (PHR or banking portal)?

2) How concerned are you about the privacy of your information in a (PHR or banking portal)?

Hypothesis 1 states that security and privacy factors concerning PHR portals would be significantly greater than those concerns surrounding online banking portals. The results suggested that the only significant difference was found for brand reputation ($t(304) = 2.90$, $p < .001$). However, these results showed that users are still more concerned with banking portals compared to PHR portals. Thus, no support was found for H1 (see Table 2 for results).

	Portal		**t(303)**
	Bank	**PHR**	
Security Perceptions			
Brand Reputation	3.88	3.74	2.90***
Signals	3.60	3.57	1.04
Privacy Perceptions			
Control Over Information	4.19	4.21	-0.69
Control Over Access	4.40	4.34	1.47
Privacy Policies	3.86	3.85	0.28
Overall Concerns			
Security Concern	2.56	2.59	-0.36
Privacy Concern	2.62	2.63	-0.32

*** p < .05, ** p < .01, *** p < 0.001**

Table 2: SPSS Mean Comparison Results

Hypotheses 2 and 3 suggest that users of online PHR portals would be concerned most with "Signals" for security (H2) and "Control over Access" for privacy (H3). The results from Table 3 show that, for security factors, brand reputation (*M=3.74*) was higher than signals (*M=3.57*). Thus, there is no support for H2. For privacy concerns, control over access had the

highest average concern (*M = 4.34*), well above both control over information (*M = 4.21*) and privacy policies (*M = 3.85*). Thus, there is support for H3.

Due to the confounding results from the entire dataset, a post-hoc analysis was conducted to understand the difference from PHR adopters and non-adopters. The secondary analysis separated the dataset into two groups: those that have already used a PHR (PHR adopters), and those that have not used a PHR (PHR non-adopters). It is important to note that unlike the analysis of the means above, the security variable "frequency of use" was omitted since the data was split by the actual use of PHR portals. Thus, the mean comparison analysis focused on the other two security factors, three privacy factors, and two questions focusing on general privacy and security concerns.

In terms of PHR adopters, 93 of 304 participants had used a PHR before. When individuals had interacted with a PHR, these individuals perceive brand, signal, privacy, and security concerns differently from bank portals. There were no significant differences concerning the privacy factors among PHR adopters. For the security factors, brand reputation was found to have the most significant difference ($t(92) = 2.86$, $p < .01$) among users in which banking portal reputation of the bank was more significant compared to the reputation of the hospital or doctor's office. Signals were also found to be significant in which signals appeared to be more important on banking portals as compared to personal health record portals ($t(92) = 2.00$, $p < .05$). Finally, users tend to have higher concerns about security and privacy on the online banking portal compared to PHRs. The results from the analysis can be found in Table 3.

	Portal		
	Bank	PHR	t (92)
Security Perceptions			
Brand Reputation	3.94	3.66	2.86**
Signals	3.71	3.61	2.00*
Privacy Perceptions			
Control Over Information	4.24	4.25	-0.09
Control Over Access	4.43	4.38	0.69
Privacy Policies	3.86	3.91	-0.67
Overall Concerns			
Security Concern	2.56	2.37	2.00*
Privacy Concern	2.57	2.35	1.92*

*** p < .05, ** p < .01**

Table 3: SPSS Mean Comparison Results – PHR Adopters

Conversely, 194 of 304 participants selected the option that they had not previously used a PHR portal and were analyzed as non-adopters. When comparing the results with the PHR adopters, all of the security and privacy factors had no significant difference when comparing the two portals. Additionally, there were no significant differences for overall security and privacy concerns. Only one variable came close (i.e. privacy concern) with non-PHR adopters tending to be more concerned with the privacy of a PHR portal when compared to an online banking portal ($t(193) = -1.83$, $p = 0.07$). The complete results for non-PHR adopters can be found in Table 4 below.

	Portal		t(194)
	Bank	PHR	
Security Perceptions			
Brand Reputation	3.86	3.80	1.17
Signals	3.57	3.57	-0.04
Privacy Perceptions			
Control Over Information	4.19	4.20	-0.43
Control Over Access	4.41	4.34	1.44
Privacy Policies	3.90	3.85	1.01
Overall Concerns			
Security Concern	2.57	2.69	-1.38
Privacy Concern	2.65	2.79	-1.83

*** p < .05, ** p < .01**

Table 4: SPSS Mean Comparison Results - Non-PHR Adopters

Physician Trust

Physician trust was also hypothesized to influence a PHR portal user's privacy and security concerns. Specifically, as trust in a user's physician increases, privacy and security concerns surrounding the use of a PHR portal will decrease (see the model in Figure 3). To examine this hypothesis, a regression was conducted using physician trust as well as the security and privacy perceptions as predictors of security concern and privacy concern. Security concern was evaluated first. Results indicate that these factors were relatively low predictors of security concern with an adjusted $R^2 = 0.06$, $F(6,297) = 4.23$, $p < 0.001$. The only significant predictor of security concern was physician trust which suggest physician trust can reduce security concerns of PHR portals. Similar results were found with privacy concern, adjusted $R^2 = 0.07$, $F(6,297) = 4.59$, $p < 0.001$. An additional factor, PHR use, was examined to understand if these factors may influence a PHR user's current or future use of the system. A similar regression was conducted with the predictors remaining the same with Use/Intent to Use being the dependent variable. Results were slightly better with an adjusted $R^2 = 0.11$, $F(6,297) = 7.40$, $p < 0.001$. Again, the only significant predictor was Physician Trust suggesting that when user's trust their physician, this trust is transferred onto the PHR portal with increased intent to start or continue portal use.

Similar to the prior analysis, the dataset was split based on current adoption or use of a PHR Portal (i.e. Adopters vs. Non-Adopters). The results can be found in Table 5. Across both adopter and non-adopters, Physician Trust again remains the only significant predictor. However, the results found that not only Physician Trust ($\beta = -0.39$, $t(86) = -3.92$, $p = 0.000$) but Signals ($\beta = -0.32$, $t(86) = -1.97$, $p = 0.05$) as well significantly impact both security and privacy concerns for users who have at least interacted with the portal previously.

	Security Concern	Privacy Concern	Continued Use
Adopters	$R^2 = 0.16$ $F(6,86) = 3.84^{**}$	$R^2 = 0.16$ $F(6,86) = 3.90^{**}$	$R^2 = 0.31$ $F(6,86) = 7.92^{***}$
Non-Adopters	$R^2 = 0.03$ $F(6,188) = 1.82$	$R^2 = 0.05$ $F(6,188) = 2.52^{*}$	$R^2 = 0.05$ $F(6,188) = 2.69^{*}$

Note: Adjusted R^2 reported
*** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$
Table 5: Regression Analysis of PHR Adopters and Non-Adopters

Qualitative Analysis

In addition to the quantitative mean comparison analyses, a qualitative analysis was conducted. As part of the survey, open-ended questions were included to allow participants to write their personal feelings toward portals as well as any additional factors that may influence their perceptions of security and privacy on the portals. Questions focused on why they did or did not use portals and other factors influencing their perceptions and were asked on the survey during the respective portal being examined (either banking or PHR).

The first question asked participants why they did not use an online banking portal. Some of the more creative answers were that they "seemed sketchy" and were "fraught with peril to average person with low knowledge of internet security [sic]." Besides these answers, others felt they were insecure, or that "it sometimes does not feel safe to access the information online," while one individual was "very careful in regard to monetary transactions online as I consider them to be high security risks."

When asked about any other security and privacy concerns that the survey did not cover, some of the security concerns were "whether or not the security certificates are up to date," "having key loggers on my own computer," and whether or not "grammar and punctuation were correctly used in the website's design." When asked about other privacy concerns, one

participant said that they would "sometimes worry about someone hacking the site" while another said they wanted to see "a good history of privacy practices."

When looking at the qualitative data for the personal health record discipline, participants were first asked why they did not use a PHR. There were a lot of responses to this question. Some responses were that "I had never heard of a PHR before! They sound very interesting, and I would certainly consider using one," "I'm not comfortable having very sensitive information about my health in a cloud-based environment. There is too much potential for this data to be breached which would lead to permanent damage," and lastly one participant said, "I prefer the old fashioned way. I like for my personal health record to be in a file cabinet or in a hospital computer filing system. I don't need that much access to my personal health record."

When asked about other PHR security concerns not addressed in the survey, one participant was worried about "the success of hackers" while one participant gave a very interesting answer that states, "I am worried about who might be able to get access to my records LEGALLY, not so much whether someone can get access to them illegally [sic]." When asked about other PHR privacy concerns not addressed in the survey, one person stated that "Even if I can currently make choices to limit who has access to my record, I would worry that in the future new rules and regulations might open my record to being viewed by interested parties whether I agree or not."

Discussion of Results

The results from the quantitative analysis of factors influencing security and privacy were unexpected. Currently, there does not appear to be significant difference in how user perceives the security and privacy of online banking portals compared to the security and privacy of personal health records. If anything, the general population is a bit more critical of online

banking portals. The analysis across the entire dataset showed that only a single factor was significantly different across the portals. This may be due to the fact that adoption is still relatively low since only 30% of participants' verified prior use. Perhaps, the general population just does not have enough of an opinion on the comparisons we were testing. It is interesting to note that in terms of the security variables, both the online banking portal and PHR had brand reputation score as the highest security variable. This shows that people still look at what the brand represents and how they conduct themselves when choosing a bank or health care provider. In addition, the online banking portal and PHR both had control over access as the highest privacy variable. This reflects that people today want control over who sees what information, and this only further strengthens the research that was presented earlier in the literature review (Caine et al., 2015; Caine & Hanania, 2013).

Another interesting result is that the banking portal scored equal to or greater than the personal health record in every security and privacy variable, but not by any significant value. A likely reason for this is because online banking portals have become more mainstream and a majority of the population (including our sample population) have assimilated them in to their daily lives and routines (e.g. they are more familiar with them). The PHR scores may have been lower due to a lack of familiarity around the features of a PHR and due to the current low adoption rate of PHRs. With the literature and our sample population reflecting the low adoption of personal health records and as more hospitals and doctors' offices move towards the digitization of their patients' health information, perhaps the results may change over time as the use of PHR become a standard practice within the medical industry (Dimitropoulos et al., 2011). With PHRs almost scoring at the same level as online banking portals with low adoption, then perhaps PHR perceptions could be different when the technology becomes more mainstream and

matures. When looking at the qualitative reasoning behind why PHR adoption was so low, reoccurring themes were that they felt that they did not need one, they did not know about them, they were not going to the doctor on a regular basis, or that their doctor's practice was not leveraging this kind of technology.

Since PHR adoption is low, a separate, quantitative mean comparison was done that split up the PHR adopters and non-PHR adopters. Like our first mean analysis, brand reputation was the most significant security factor. This helps further strengthen the conclusion that brand reputation (whether it be a banking institution or healthcare network) is a significant factor that individuals consider when using an online banking portal or PHR. Specifically, PHR adopters tend to consider the brand reputation of the bank more than the brand reputation of the hospital network or doctor's office. In addition to brand reputation, the variables of website signals, security concerns, and privacy concerns were also deemed to be significant factors. For website signals, PHR adopters tend to consider the website signals of the banking portal to be more significant than the website signals on a PHR. Lastly, for security and privacy concerns, these also concluded that PHR adopters tend to consider their security and privacy concerns more when using an online banking portal compared to their PHR. In essence, for PHR adopters, they tend to consider brand reputation, website signals, their security concerns, and their privacy concerns more for banking portals than their PHRs. This aligns with the results of our first mean analysis where banking portals scored at or above with PHRs in every variable. In addition, the mean values were not significantly different as with the first mean analysis above.

For the non-PHR adopters, it was stated that none of the variables seem to have any significance when compared to those that use a PHR. A reason for this may be because they are not familiar with a PHR and their features. However, while no conclusions can be made as to

what the participants significantly value, early outlook shows that the most promising variable to become significant is the privacy concern variable. As non-adopters consider becoming adopters, they're most likely to be concerned about the privacy of their health information within a PHR over banking information in an online banking portal. The second most promising variable is another privacy variable, "Control over Information." While the privacy concern variable scored more towards the PHR side, the "Control over Information" variable leans more towards the banking portal side. Thus, non-PHR adopters may be more concerned with controlling their banking information over their health information. Lastly, the security concern variable is also promising. Like the privacy concern variable, this one leaned more towards the PHR side, thus non-PHR adopters may be more concerned about the security of their health information in a PHR when compared to the banking information in an online banking portal. It is interesting to note that while the security and privacy concern variables scored more towards the PHRs amongst PHR adopters, these two variables scored more towards the online banking portals amongst non-PHR adopters. In essence, their privacy concerns, control over information, and their security concerns are likely to be variables that non-PHR adopters may deem significant when they do adopt a PHR.

Another part of this research was to determine how physician trust influenced privacy and security concerns and whether it had any impact on adoption. Based on the linear regression results in Table 6, if patients trust their primary care provider, then their concerns around security and privacy tend to be lower, and they are more likely to adopt a PHR. This is an interesting conclusion as this reinforces that patients tend to put a lot of trust in to their physician, and they may not only trust just their medical treatments but their opinions on PHRs and technology as well. This creates a domino-like effect, because with physicians being more

critical towards the idea of a PHR, this may be a reason as to why PHR adoption is so low. If patients trust their physician and the physician endorses a PHR, then they feel more comfortable with the idea and will likely use one for themselves; if the trust relationship is not that strong, then the patients may not feel as comfortable and are not as likely to use one, thus hindering the PHR adoption rate. Lastly, with these findings, it seems that people are replacing the brand reputation of the hospital or physician's office with the professional relationship between themselves (the patient) and the physician. However, the brand reputation factor still adheres to online banking portals as most people tend to look at the bank brand's reputation as a whole rather than the relationship between a customer and a specific banker. Thus for PHRs, the personal relationship between a physician and a patient seems to trump the brand reputation of the hospital or physician's office.

Lastly, when looking at the quantitative analyses that have been conducted, it is evident that people still have security, privacy, and trust concerns. However, when looking at the qualitative answers that participants wrote, some of their comments were suggestions of what they would like to see in future iterations of online portals – whether it be a banking portal or PHR. In order to help mitigate concerns in the future, some participants left suggestions as to what the designers behind these technologies can do to ease their security and privacy concerns in future releases.

From both the quantitative and qualitative analysis, the following are design recommendations and suggestions to reduce user concerns around privacy and security of PHR portals:

- Authentication controls: multi-factor authentication, biometrics, and word/number (also known as captchas)

- Periodic password changes
- User alerts: alerting a user when someone accesses their account
- Security questions
- Certificate authorities and HTTPS protection
- Visible security and privacy policies
- Allow users to set who can see what sets of their health information and for a specific duration of time
- Updated technology

Of the users that wrote in implementing updated technology, they did not specify what they would specifically like to see. If designers and developers considered implementing some of the suggested features (if they have not done so already) then perhaps this would ease the general user's security and privacy concerns. This serves as another potential reason for future work. As the technology in these portals is enhanced in the coming years, then maybe the perceptions of the general population will be different.

CHAPTER 5: CONCLUSION AND FUTURE WORK

Conclusion

The goal of this study was to determine if there are differences in security and privacy perceptions between online banking portals and personal health records. To reiterate, personal health records are a type of portal that contains a patient's medical that is primarily provided directly from the patient, but their physician can add information accordingly as well. They differ from electronic health records as EHRs are more physician and medical staff-centric (meaning medical staff populate most of the data in an EHR), and personal health records are more patient-centric. Through the use of a survey dispersed to the general public and analyzing their quantitative and qualitative answers, it was determined that the differences in how they perceive these two technologies is not drastically different. Reasons for the lack of differences in the results could be due to the still low adoption rate of PHRs or because the general population may not be all that familiar with the concept of a PHR and its features. When it came to design recommendations, users wanted to see authorization control enhancements such as captchas or security questions, as well as other features such as periodic password changes and user alerts (e.g. notifying a user that they have logged in or accessed their account).

Future Work

As stated in the discussion, there are a couple of different avenues that could be used if future work wanted to be conducted. With our reason being that perceptions are not drastically different due to the low adoption rate of PHRs, perhaps this study – or a similar one – could be conducted in five or ten years. By this point, PHRs may be more mainstream and the population perceptions may be different than the results reported here. Another reason for future work may come as the technology enhancements of these online portals keeps improving. In the qualitative

results, the population left comments of what they would like to see in online portals in order to help alleviate any security or privacy concerns. If software designers take these recommendations and implement a few – if they have not done so already – then this study or a similar one could be conducted at another point in time and yield different results.

REFERENCES

Al Abdulwahid, Abdulwahid, et al. "Security, Privacy and Usability–A Survey of Users' Perceptions and Attitudes." Trust, Privacy and Security in Digital Business. Springer International Publishing, 2015. 153-168.

Anderson, Catherine L., and Ritu Agarwal. "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions." MIS Quarterly 34.3 (2010): 613-643.

Bhattacherjee, Anol. "Individual trust in online firms: Scale development and initial test." Journal of Management Information Systems 19.1 (2002): 211-241.

Boss, Scott R., et al. "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security." European Journal of Information Systems 18.2 (2009): 151-164.

Caine, Kelly, et al. "Designing a patient-centered user interface for access decisions about EHR data: Implications from patient interviews." Journal of General Internal Medicine 30.1 (2015): 7-16.

Caine, Kelly, and Rima Hanania. "Patients want granular privacy control over health information in electronic medical records." Journal of the American Medical Informatics Association 20.1 (2013): 7-15.

Campos-Castillo, Celeste, and Denise L. Anthony. "The double-edged sword of electronic health records: implications for patient disclosure." Journal of the American Medical Informatics Association 22.e1 (2015): e130-e140.

Carlos Roca, Juan, Juan José García, and Juan José de la Vega. "The importance of perceived trust, security and privacy in online trading systems." Information Management & Computer Security 17.2 (2009): 96-113.

Casalo, Luis V., Carlos Flavián, and Miguel Guinalíu. "The role of security, privacy, usability and reputation in the development of online banking." Online Information Review 31.5 (2007): 583-603.

Chan, Mark, Irene Woon, and Atreyi Kankanhalli. "Perceptions of information security in the workplace: linking information security climate to compliant behavior." Journal of Information Privacy and Security 1.3 (2005): 18-41.

Childs, Dan, Haeree Chang, Audrey Grayson, and ABC News Medical Unit. "President-Elect Urges Electronic Medical Records in 5 Years." ABC News. ABC News Network, 09 Jan. 2009. Web. 29 Oct. 2015.

Dimitropoulos, Linda, et al. "Public attitudes toward health information exchange: perceived benefits and concerns." The American Journal of Managed Care 17.12 Spec No. (2011): SP111-6.

Emani, Srinivas, et al. "Patient perceptions of a personal health record: a test of the diffusion of innovation model." Journal of Medical Internet Research 14.6 (2012).

Gaylin, Daniel S., et al. "Public attitudes about health information technology, and its relationship to health care quality, costs, and privacy." Health Services Research 46.3 (2011): 920-938.

Hoffman, Donna L., and Thomas P. Novak. "Trustbuilders vs trustbusters." The Industry Standard, May 11 (1998).

Jahangir, Nadim, and Noorjahan Begum. "The role of perceived usefulness, perceived ease of use, security and privacy, and customer attitude to engender customer adaptation in the context of electronic banking." African Journal of Business Management 2.2 (2008): 32.

Kim, Changsu, et al. "An empirical study of customers' perceptions of security and trust in e-payment systems." Electronic Commerce Research and Applications 9.1 (2010): 84-95.

Kolodinsky, Jane M., Jeanne M. Hogarth, and Marianne A. Hilgert. "The adoption of electronic banking technologies by US consumers." International Journal of Bank Marketing 22.4 (2004): 238-259.

Luchenski, Serena, et al. "Survey of patient and public perceptions of electronic health records for healthcare, policy and research: study protocol." BMC Medical Informatics and Decision Making 12.1 (2012): 40.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model." Information Systems Research 15.4 (2004): 336-355.

McFadzean, Elspeth, Jean-Noel Ezingeard, and David Birchall. "Perception of risk and the strategic impact of existing IT on information security strategy at board level." Online Information Review 31.5 (2007): 622-660.

Patel, Vaishali, et al. "The Role of Health Care Experience and Consumer Information Efficacy in Shaping Privacy and Security Perceptions of Medical Records: National Consumer Survey Results." JMIR Medical Informatics 3.2 (2015).

Patel, Vaishali, J. D. Lucia Savage, and Wesley Barker. "Individuals' Perceptions of the Privacy and Security of Medical Records."

Pikkarainen, Tero, et al. "Consumer acceptance of online banking: an extension of the technology acceptance model." Internet Research 14.3 (2004): 224-235.

Ray, Soumya, Terence Ow, and Sung S. Kim. "Security assurance: How online service providers can influence security control perceptions and gain trust." Decision Sciences 42.2 (2011): 391-412.

Roboff, Gary, and Cheryl Charles. "Privacy of financial information in cyberspace: banks addressing what consumers want." Journal of Retail Banking Services 20.3 (1998): 51-57.

Sathye, Milind. "Adoption of Internet banking by Australian consumers: an empirical investigation." International Journal of Bank Marketing 17.7 (1999): 324-334.

Teer, Faye P., S. E. Kruck, and Gregory P. Kruck. "Empirical Study of Students' Computer Security-Practices/Perceptions." Journal of Computer Information Systems 47.3 (2007): 105.

Thom, David H., et al. "Further validation and reliability testing of the Trust in Physician Scale." Medical Care 37.5 (1999): 510-517.

Weir, Catherine S., et al. "User perceptions of security, convenience and usability for ebanking authentication tokens." Computers & Security 28.1 (2009): 47-62.

Weiss, Irving. "EHR vs EMR - Definition, Benefits and Usage Trends Practice Fusion." Practice Fusion Blog. Practice Fusion, Inc., 18 Sept. 2015. Web. 30 Oct. 2015.

Wen, Kuang-Yi, et al. "Consumers' perceptions about and use of the internet for personal health records and health information exchange: analysis of the 2007 Health Information National Trends Survey." Journal of Medical Internet Research 12.4 (2010).

Witry, Matthew J., et al. "Family physician perceptions of personal health records." Perspectives in health information management/AHIMA, American Health Information Management Association 7.Winter (2010).

APPENDIX A

Pilot Study Results

APPENDIX A

Preliminary Pilot Study Results

In total, we had a sample size of 55 participants. Approximately 71% of the participants were between the ages of 18-24, approximately 24% were among the ages of 25-34, and the other 5% were older than 35. In terms of gender, it was almost an even split. Approximately 51% of participants were male, approximately 46% were female, and the other 3% chose not to disclose their gender. Generally, 93% of participants use the Internet daily, and 7% use the Internet often. The table below (Table A1) shows some other statistics around how often they use PHRs while on the Internet and how many hours per day they use the Internet. It is interesting to note that over half of the participants (69%) never or rarely have accessed their PHR on the Internet. While almost the majority of participants spend about 5 – 7 hours online, very few are looking at their PHR during that time.

Statistics Around Internet Usage			
How Often Participants Accessed PHR on Internet		**How Many Hours Per Day Participants Spend Online**	
Never	25%	Less than 1 Hour	4%
Rarely	44%	2 – 4 Hours	33%
Sometimes	27%	5 – 7 Hours	44%
Often	2%	8 – 10 Hours	15%
Daily	2%	11+ Hours	5%

Table A1: Internet Usage Statistics of Pilot Study Participants

A large majority of the survey discussed privacy and security concerns around online banking portals and personal health records. In terms of how concerned the participants were about the security and privacy of online banking portals and on a scale of one to five, the participants scored a 2.7 and 2.8, respectively. In terms of how concerned the participants were about the security and privacy of personal health records, the participants scored a 2.6 and 2.8, respectively. A possible explanation as to why the online banking portal scores were low would be that this type of portal is more established, allowing the public to become more comfortable with them; a possible explanation as to why the PHR scores were low would be because a

majority of the participants, over 60%, had never used a PHR, inferring that the scores were low because the majority of the participants were not familiar with a PHR.

The study also asked the participants questions around specific areas of security, as noted in our methodology model. The results comparing the two areas are shown in Figure A1. The two biggest differences were around the URL beginning with "https://," and whether the portal prompted them for a username and password. The participants scored .47 points more towards the PHR beginning with "https://" compared to the online banking portal, and the participants scored .51 points more towards the online banking portal prompting a username and password compared to the PHR. The questions with minimal differences were around the portal having a professional look and feel, and using the portal every day. The participants scored .07 points more towards the PHR having a professional look and feel when compared to the online banking portal, and the participants scored .09 points more towards the online banking portal being used every day when compared to the PHR. Based on these preliminary results, it can be determined that when it comes to security, participants are most concerned with an online banking portal requiring a strong username and password, as this area scored the highest with a 4.42. In terms of PHR security, participants are most concerned with the URL beginning with "https://," as this area scored the highest with a 4.33.

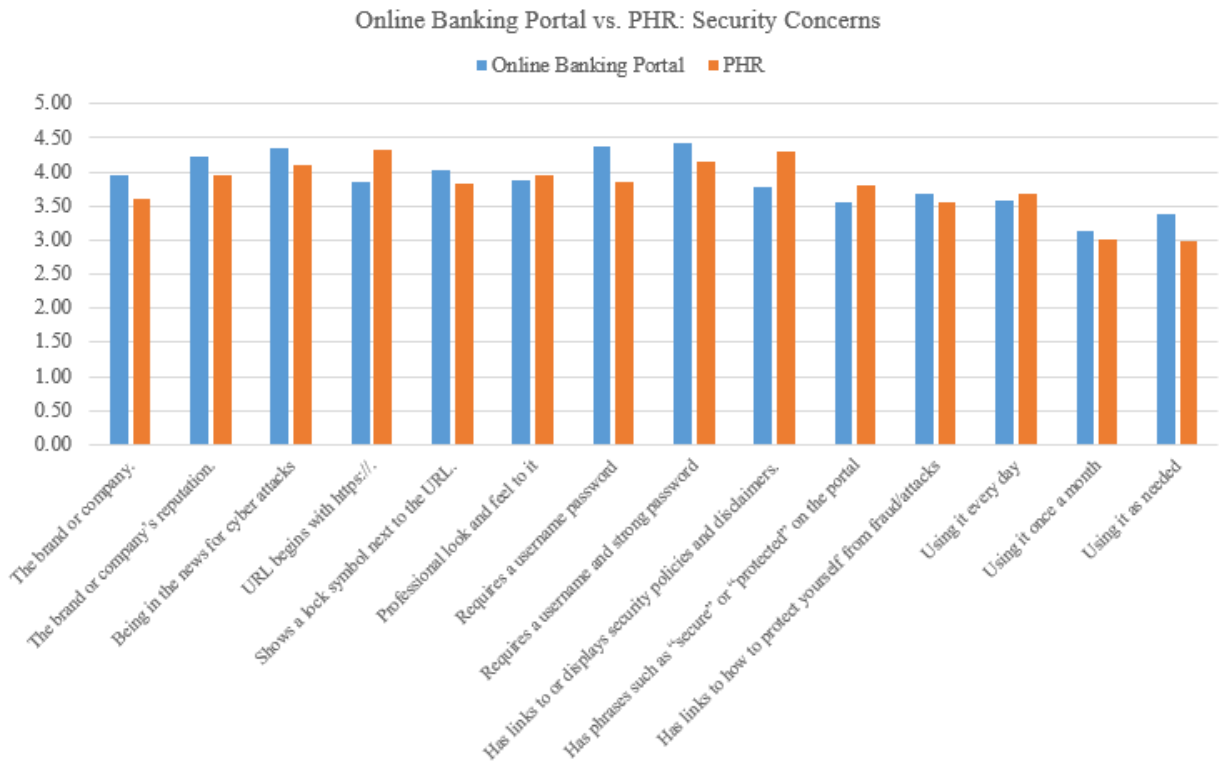


Figure A1: Online Banking Portal vs. PHR: Security Concerns

Lastly, the study asked participants questions concerning specific areas of privacy. The results comparing the two areas are shown in Figure A2. The two biggest differences were around being able to decide what information to disclose and being able to hide sensitive information. The participants scored .13 points higher on being able to decide what information to disclose on an online banking portal when compared to a PHR, and the participants scored .18 points more on being able to hide sensitive information in an online banking portal when compared to a PHR. The most minimal differences were around no one being able to see their information unless authorized and deciding how long to disclose information to others. The participants scored .02 points higher on no one being able to see their information unless authorized on a PHR when compared to a banking portal, and the participants scored .02 points higher on deciding how long to disclose information to others on a banking portal when

compared to a PHR.

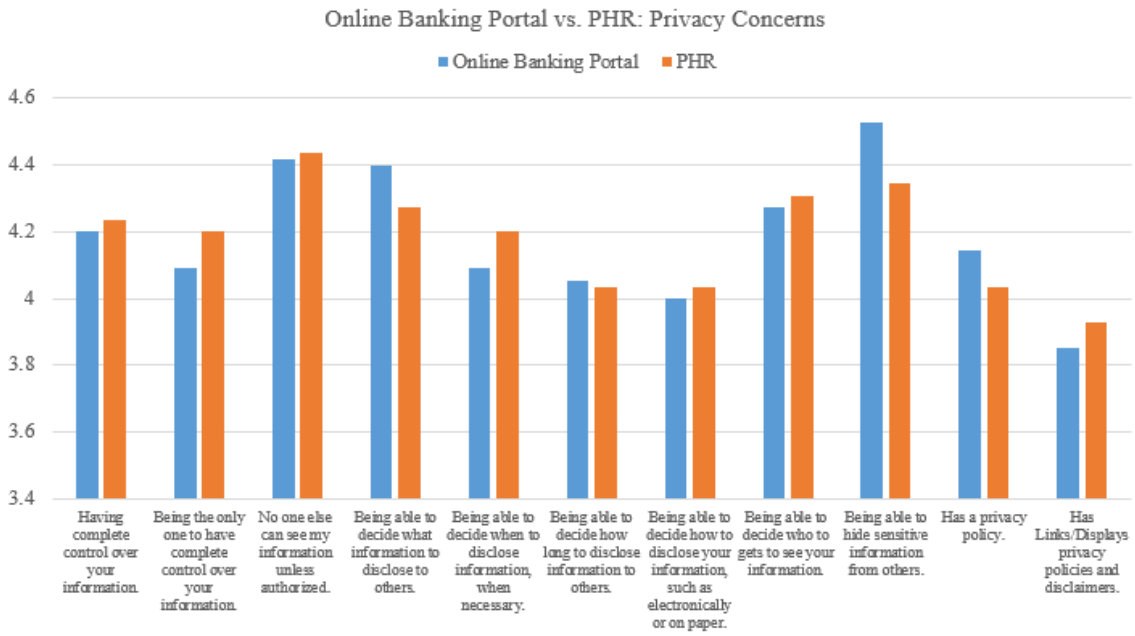


Figure A2: Online Banking Portal vs. PHR: Privacy Concerns

These initial results suggest that when it comes to privacy, participants are most concerned with being able to hide sensitive information from an employee when it comes to an online banking portal, as this area scored the highest with a 4.53. In terms of PHR privacy, participants are most concerned with only authorized personnel being able to view information, as this area scored the highest with a 4.44.

APPENDIX B

Final Survey (with changes from pilot study)

APPENDIX B

PHR Perceptions - Version 2 (version sent out to participants)

You are being invited to participate in a research study titled Perceptions of Online Personal Health Records. This study is being done by researchers from the University of North Carolina Wilmington. The purpose of this research study is to understand an individual's perception of the websites used to access online information such as banking and personal healthcare records. If you agree to take part in this study, you will be asked to complete an online survey/questionnaire. This survey/questionnaire will ask about your security perceptions of a few common websites that allow users to bank or look up health records and it will take you approximately 10 minutes to complete. The questions do not ask for any personally identifiable information and pose no risk to the user answering the questions. Your participation in this study is voluntary. However, please be aware that you will only receive payment if you complete the entire survey. The data you provide will be kept secure once it is in the researcher's possession. However, the researcher cannot guarantee security during transmission of data due to keylogging or other spyware that may exist on the computer you are using. By continuing the survey you are indicating that you are at least 18 years old, have read and understood this consent form and agree to participate in this research study.

Please Indicate Your Age (Must be 18 or Older) (Round down to the nearest year).

- ❍ 17 or Under
- ❍ 18-24
- ❍ 25-34
- ❍ 35-44
- ❍ 45-54
- ❍ 55-64
- ❍ 65+

Please Indicate Your Ethnicity.

- ❍ African American/Black
- ❍ American Indian/Alaska Native
- ❍ Asian
- ❍ Native Hawaiian/Other Pacific Islander
- ❍ White Caucasian
- ❍ Hispanic/Latino
- ❍ Other _____
- ❍ I prefer not to answer.

Please Indicate Your Gender.

- ❍ Male
- ❍ Female
- ❍ Other _____
- ❍ I prefer not to answer.

Please Indicate Your Highest Completed Level of Education.

- ❍ Some High School/GED
- ❍ High School Diploma/GED Graduate
- ❍ Some College
- ❍ Associate's Degree
- ❍ Bachelor's Degree
- ❍ Doctoral Degree
- ❍ I prefer not to answer.

Please Indicate Your Income.

- ❍ <$20,000
- ❍ $20,000-$39,999
- ❍ $40,000-$59,999
- ❍ $60,000-$79,999
- ❍ $80,000-$99,999
- ❍ $100,000+
- ❍ I prefer not to answer.

How Often Do You Access the Internet?

- ❍ Never
- ❍ Rarely
- ❍ Sometimes
- ❍ Often
- ❍ Daily

How Often Do You Use the Internet for the Following?

	Never	Rarely	Sometimes	Often	Daily	N/A
Online shopping (e.g. Amazon, Zappos)	❍	❍	❍	❍	❍	❍
Paying bills	❍	❍	❍	❍	❍	❍
Watching videos (e.g. YouTube, Vevo, etc.)	❍	❍	❍	❍	❍	❍
Streaming videos, movies, TV shows (e.g. Netflix, Hulu)	❍	❍	❍	❍	❍	❍
Streaming or listening to music (e.g. Spotify, Pandora, Apple Music)	❍	❍	❍	❍	❍	❍
Email	❍	❍	❍	❍	❍	❍
Social media (e.g. Facebook, Twitter, LinkedIn, Instagram)	❍	❍	❍	❍	❍	❍
Viewing your health information in a Personal Health Record (PHR)	❍	❍	❍	❍	❍	❍
Research/Productivity/School Assignments	❍	❍	❍	❍	❍	❍
News	❍	❍	❍	❍	❍	❍
Other (if you do not have an Other, select "N/A")	❍	❍	❍	❍	❍	❍

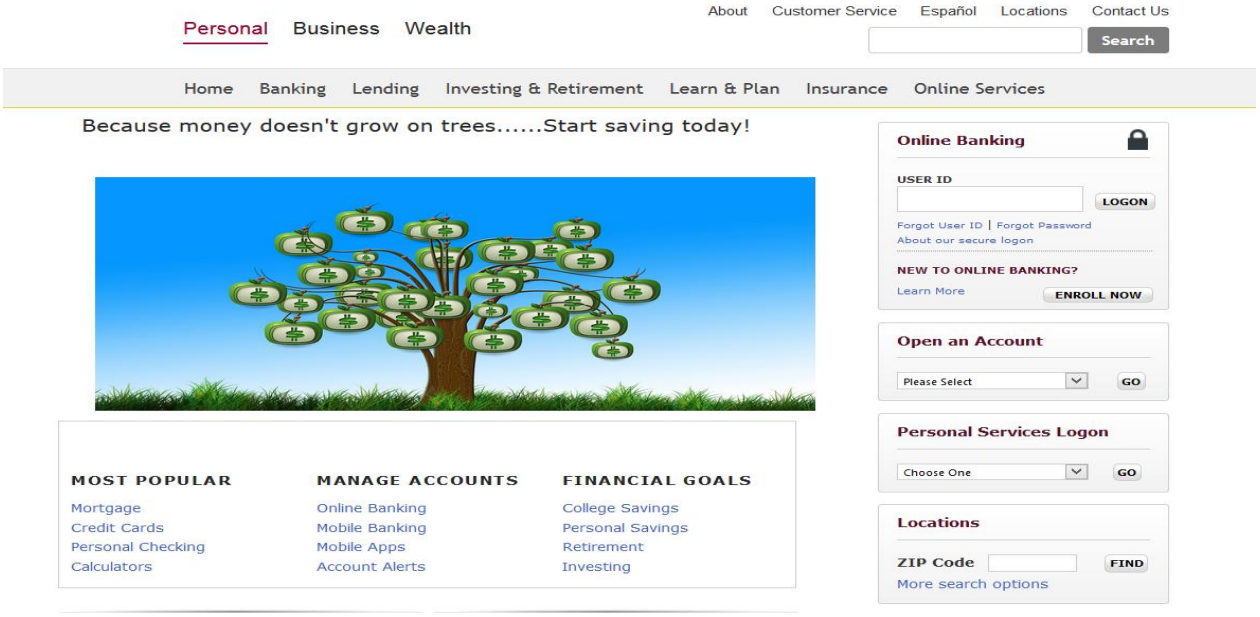
How Many Hours per Day do You Spend Online? (Round up to the nearest hour)

- ❍ Less than 1 Hour
- ❍ 2-4 Hours
- ❍ 5-7 Hours
- ❍ 8-10 Hours
- ❍ 11+ Hours

Please answer the questions below about your feelings towards trust.

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
It is easy for me to trust a person or thing.	❍	❍	❍	❍	❍
I tend to trust a person or thing, even though I have little knowledge of it.	❍	❍	❍	❍	❍
Trusting someone or something is not difficult.	❍	❍	❍	❍	❍

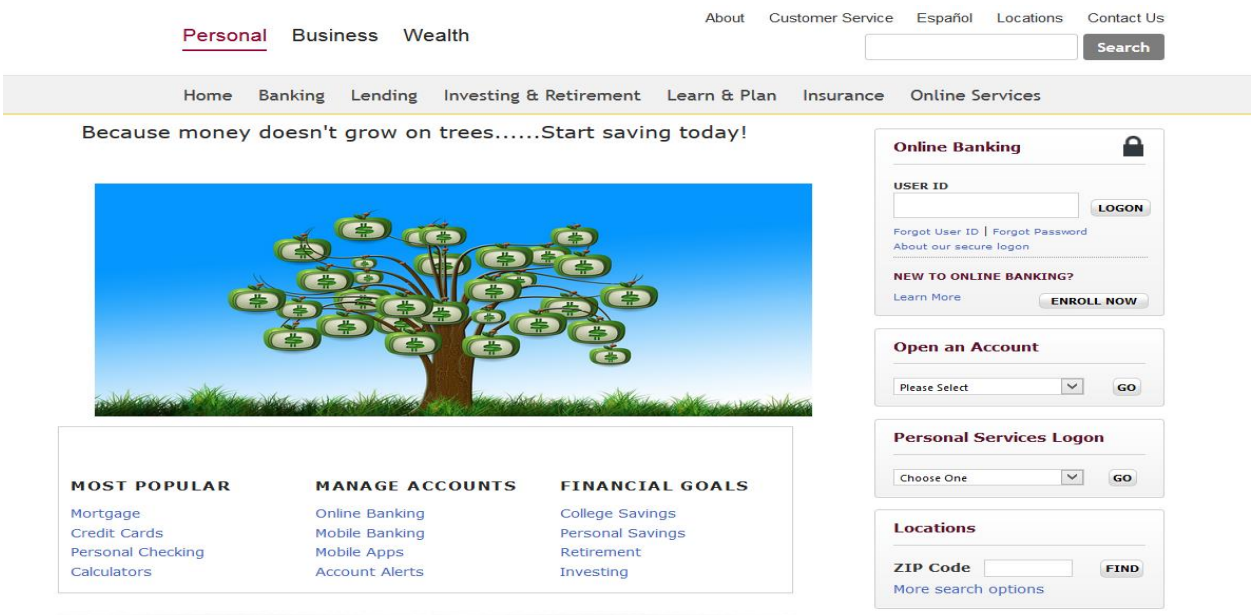
Please study the following screenshot and answer the questions that follow.



Have you used an online banking portal similar to the one shown above?

- ❍ Yes
- ❍ No
- ❍ I am not sure
- ❍ I prefer not to answer

Why don't you use an online banking portal?



Security defined: Safe-guarding data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.

Based on the screenshot and information security definition given, how concerned are you about the security of your information in an online banking portal like the one shown above?

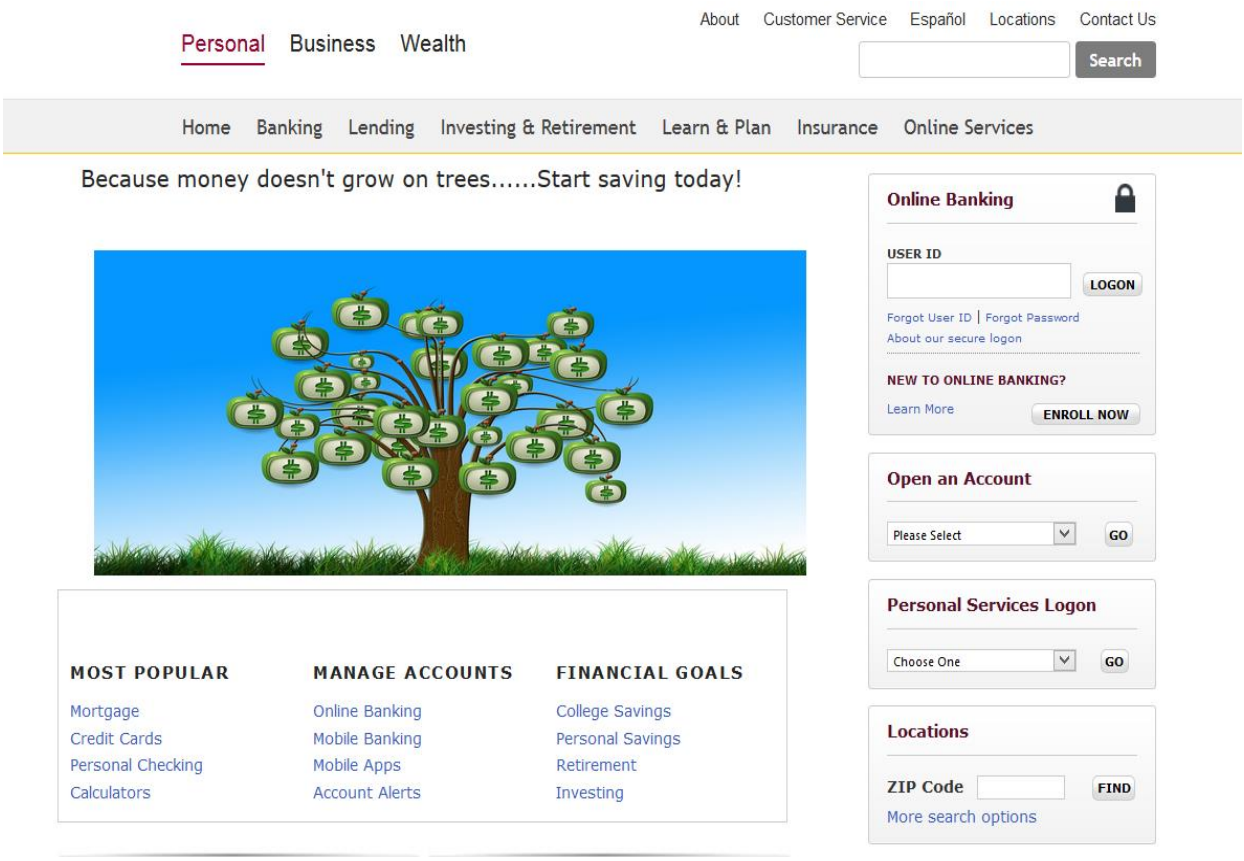
- ❍ Not at all concerned
- ❍ Slightly concerned
- ❍ Moderately concerned
- ❍ Very concerned
- ❍ Extremely concerned

Please indicate how much the following factors influence your feelings on how secure your information is:

	Not at all influential	Slightly influential	Somewhat influential	Very influential	Extremely influential
The brand or company.	❍	❍	❍	❍	❍
The brand or company's reputation.	❍	❍	❍	❍	❍
The brand or company being in the news for an information breach/breaches.	❍	❍	❍	❍	❍
The online banking portal URL begins with https://.	❍	❍	❍	❍	❍
The online banking portal show a lock symbol next to the URL.	❍	❍	❍	❍	❍
The online banking portal has a professional look and feel to it, and it is obvious that the company has invested in the online banking portal.	❍	❍	❍	❍	❍
The online banking portal requires a non-strong username and password for your account.	❍	❍	❍	❍	❍
The online banking portal requires a username and strong password for your account.	❍	❍	❍	❍	❍

The online banking portal has links to or displays security policies and disclaimers.	❍	❍	❍	❍	❍
The online banking portal has phrases such as “secure” or “protected” around their online banking portal.	❍	❍	❍	❍	❍
The online banking portal has links to how to protect yourself from fraud and other cyber-attacks.	❍	❍	❍	❍	❍
Using the online banking portal every day	❍	❍	❍	❍	❍
Using the online banking portal once a month	❍	❍	❍	❍	❍
Using the online banking portal as needed	❍	❍	❍	❍	❍

Q19 Please describe any other security concerns you have that were not addressed in the above questions.



Privacy defined: the right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed.

Based on the screenshot and privacy definition given, how concerned are you about the privacy of your information in an online banking portal like the one shown above?

- ❍ Not at all concerned
- ❍ Slightly concerned
- ❍ Moderately concerned
- ❍ Very concerned
- ❍ Extremely concerned

Please indicate how much the following factors influence your feelings on how private your information is:

	Not at all influential	Slightly influential	Somewhat influential	Very influential	Extremely influential
Having complete control over your information.	❍	❍	❍	❍	❍
Being the only one to have complete control over your information.	❍	❍	❍	❍	❍
No one else can see my information unless authorized.	❍	❍	❍	❍	❍
Being able to decide what information to disclose to others.	❍	❍	❍	❍	❍
Being able to decide when to disclose information, when necessary.	❍	❍	❍	❍	❍
Being able to decide how long to disclose information to others.	❍	❍	❍	❍	❍
Being able to decide how to disclose your information, such as electronically or on paper.	❍	❍	❍	❍	❍

Being able to decide who to gets to see your information.	❍	❍	❍	❍	❍
Being able to hide sensitive information from others.	❍	❍	❍	❍	❍
The online banking portal has a privacy policy.	❍	❍	❍	❍	❍
The online banking portal has links to or displays privacy policies and disclaimers.	❍	❍	❍	❍	❍

Please describe any other privacy concerns you have that were not addressed in the above questions.

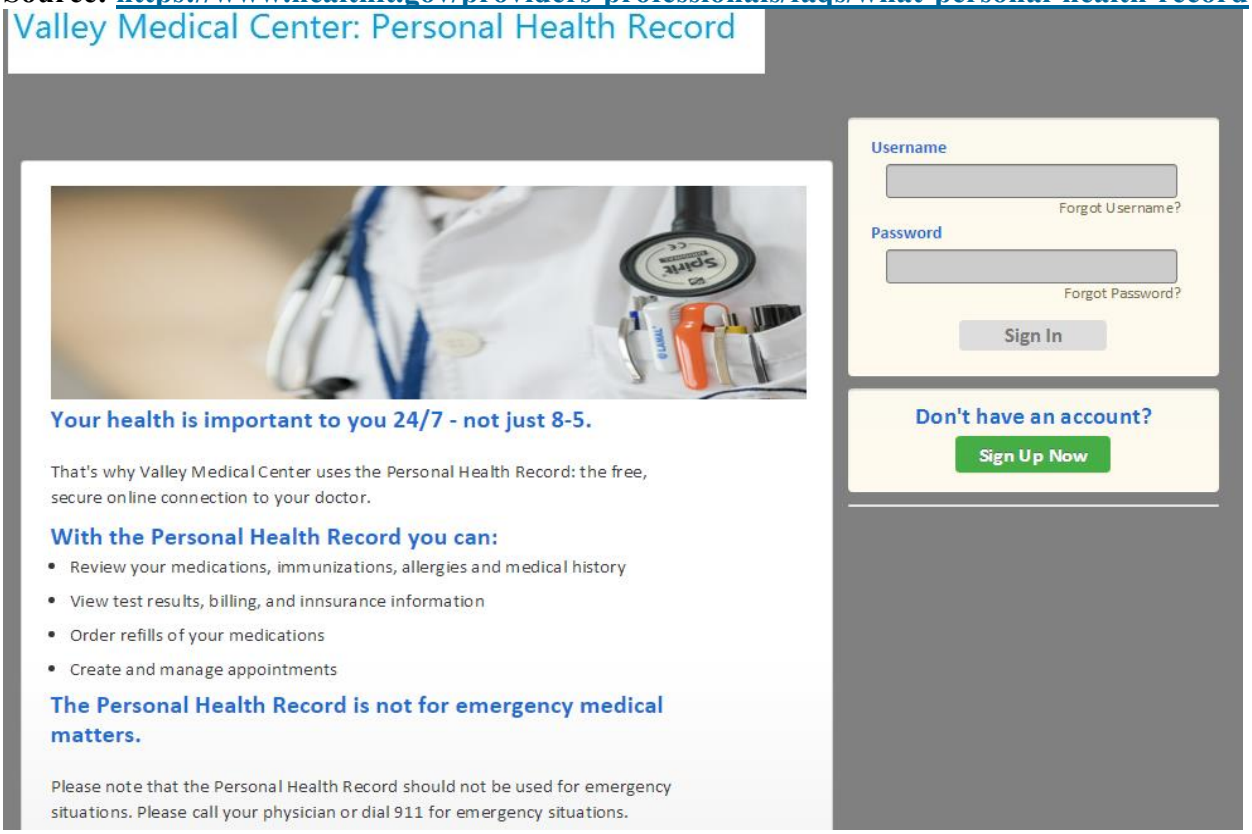
Please study the following screenshot and definition and answer the questions that follow.

Personal Health Record (PHR) defined: A personal health record (PHR) is an electronic application used by patients to maintain and manage their health information in a private, secure, and confidential environment.

PHRs:

- **Are managed by patients**
- **Can include information from a variety of sources, including health care providers and patients themselves**
- **Can help patients securely and confidentially store and monitor health information, such as diet plans or data from home monitoring systems, as well as patient contact information, diagnosis lists, medication lists, allergy lists, immunization histories, and much more**
- **Are separate from, and do not replace, the legal record of any health care provider Are distinct from portals that simply allow patients to view provider information or communicate with providers**

Source: https://www.healthit.gov/providers-professionals/faqs/what-personal-health-record



Have you used a PHR like the one shown above?

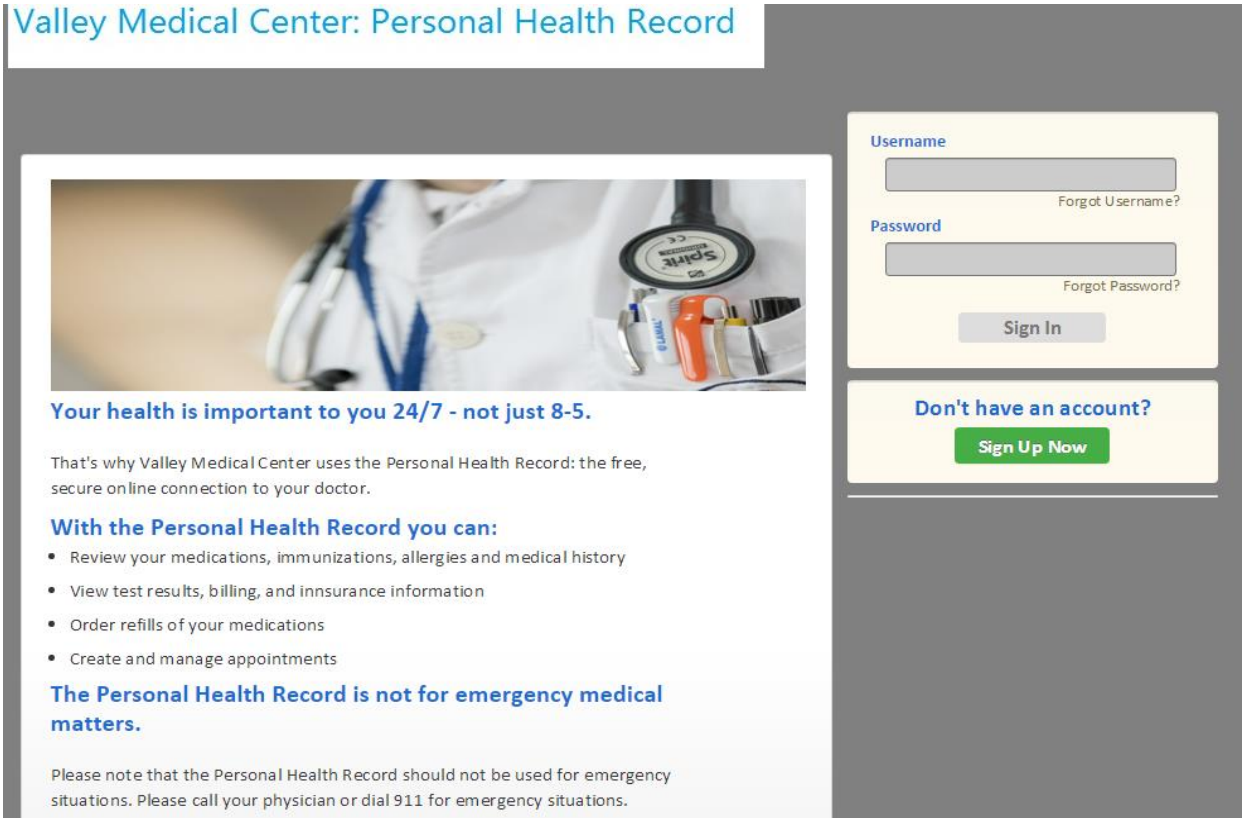
- ❍ Yes
- ❍ No
- ❍ I am not sure
- ❍ I prefer not to answer

Why don't you use a PHR?

Please state how much you agree or disagree with the following statements about your physician.

	Strongly disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
I doubt that my doctor really cares about me as a person.	❍	❍	❍	❍	❍
My doctor is usually considerate of my needs and puts them first.	❍	❍	❍	❍	❍
I trust my doctor so much that I always try to follow their advice.	❍	❍	❍	❍	❍
If my doctor tells me something is so, then it must be true.	❍	❍	❍	❍	❍
I sometimes distrust my doctor's opinions and would like a second one.	❍	❍	❍	❍	❍
I trust my doctor's judgments about my medical care.	❍	❍	❍	❍	❍
I feel my doctor does not do everything they should about my medical care.	❍	❍	❍	❍	❍

I trust my doctor to put my medical needs above all other considerations when treating my medical problems.	❍	❍	❍	❍	❍
My doctor is well qualified to manage (diagnose and treat or make an appropriate referral) medical problems like mine.	❍	❍	❍	❍	❍
I trust my doctor to tell me if a mistake was made about my treatment.	❍	❍	❍	❍	❍



Security defined: Safe-guarding data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.

Based on the screenshot and information security definition given, how concerned are you about the security of your information in a PHR like the one shown above?

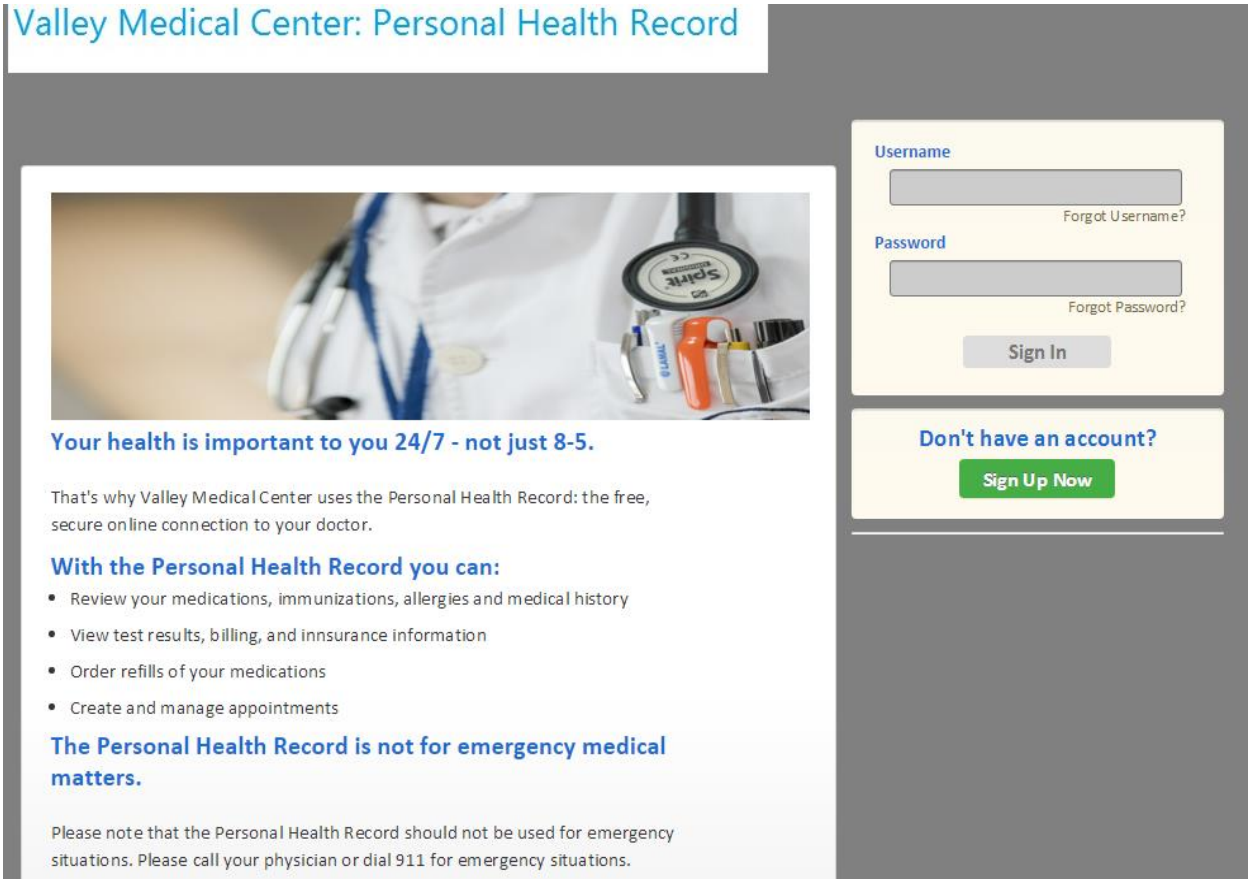
- ❍ Not at all concerned
- ❍ Slightly concerned
- ❍ Moderately concerned
- ❍ Very concerned
- ❍ Extremely concerned

Please indicate how much the following factors influence your feelings on how secure your information is:

	Not at all influential	Slightly influential	Somewhat influential	Very influential	Extremely influential
The brand or hospital.	❍	❍	❍	❍	❍
Your physician	❍	❍	❍	❍	❍
The brand or hospital's reputation.	❍	❍	❍	❍	❍
The brand or hospital being in the news for an information breach/breaches.	❍	❍	❍	❍	❍
The PHR URL begins with https://.	❍	❍	❍	❍	❍
The PHR show a lock symbol next to the URL.	❍	❍	❍	❍	❍
The PHR has a professional look and feel to it, and it is obvious that the company has invested in the PHR.	❍	❍	❍	❍	❍
The PHR requires a non-strong username and password for your account.	❍	❍	❍	❍	❍
The PHR requires a username and strong password for your account.	❍	❍	❍	❍	❍
The PHR has links to or displays security policies and disclaimers.	❍	❍	❍	❍	❍
The PHR has phrases such as	❍	❍	❍	❍	❍

"secure" or "protected" around their PHR.					
The PHR has links to how to protect yourself from fraud and other cyber-attacks.	❍	❍	❍	❍	❍
Using the PHR every day	❍	❍	❍	❍	❍
Using the PHR once a month	❍	❍	❍	❍	❍
Using the PHR as needed	❍	❍	❍	❍	❍

Please describe any other security concerns you have that were not addressed in the above questions.



Privacy defined: the right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed.

Based on the screenshot and privacy definition given, how concerned are you about the privacy of your information in a PHR like the one shown above?

- ❍ Not at all concerned
- ❍ Slightly concerned
- ❍ Somewhat concerned
- ❍ Very concerned
- ❍ Extremely concerned

Please indicate how much the following factors influence your feelings on how private your information is:

	Not at all influential	Slightly influential	Somewhat influential	Very influential	Extremely influential
Having complete control over your information.	❍	❍	❍	❍	❍
Being the only one to have complete control over your information.	❍	❍	❍	❍	❍
No one else can see my information unless authorized.	❍	❍	❍	❍	❍
Being able to decide what information to disclose to others.	❍	❍	❍	❍	❍
Being able to decide when to disclose information, when necessary.	❍	❍	❍	❍	❍
Being able to decide how long to disclose information to others.	❍	❍	❍	❍	❍
Being able to decide how to disclose your information, such as electronically or on paper.	❍	❍	❍	❍	❍

Being able to decide who to gets to see your information.	❍	❍	❍	❍	❍
Being able to hide sensitive information from others.	❍	❍	❍	❍	❍
The PHR has a privacy policy.	❍	❍	❍	❍	❍
The PHR has links to or displays privacy policies and disclaimers.	❍	❍	❍	❍	❍

Please describe any other privacy concerns you have that were not addressed in the above questions.

Please provide your feelings about using a portal to access your health records.

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
I would use online health records to access medical information in the future.	❍	❍	❍	❍	❍
I would strongly recommend others use health records as a convenient way to access their records.	❍	❍	❍	❍	❍
I would access health records more frequently if they were available through an online portal.	❍	❍	❍	❍	❍