SUMMARY OF IDENTITY PROOFING PRACTICES FOR PERSONAL HEALTH RECORDS OFFERING NETWORK-BASED VALUE-ADDED SERVICES

February 14, 2007

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

INTRODUCTION

This paper summarizes research performed in the area of consumer identity proofing by Personal Health Record (PHR) providers that have no prior relationship with a health care consumer. Overall, fifty (50) providers of PHRs were covered in this research. Furthermore, the research is based solely on public information available from company web sites. The types of providers researched fall into one of the following two categories:

- Off-line PHR Providers – Providers offering PHR products and applications that are operated and maintained on the patients' personal computing systems, or that can be carried by the patients (e.g., in a wallet, on a key chain). These PHRs are not capable of being connected into a network environment (e.g., over the Internet).
- On-line PHR Providers – Providers offering Internet-based, on-line services for patients to create and manage their PHRs and PHR accounts. These PHRs are either 1) completely hosted by the on-line PHR provider, or 2) locally managed by the consumer using a product or application provided by the PHR provider, but the PHR can be connected into a networked environment (e.g., over the Internet) to obtain additional services.

Figure 1 describes the breakdown between off-line and on-line PHR providers. Thirty-four percent (34%) of the providers researched, seventeen (17) providers in total, offered PHRs in an off-line only capability (i.e., non-networked); the remaining thirty-three (33) providers, sixty-six percent (66%), offered PHRs via an on-line service over the Internet where the provider hosted the PHR on behalf of the consumer, or where the consumer could network a locally managed PHR to obtain additional on-line services (e.g., synchronize with an on-line PHR account, send medical information to a provider).

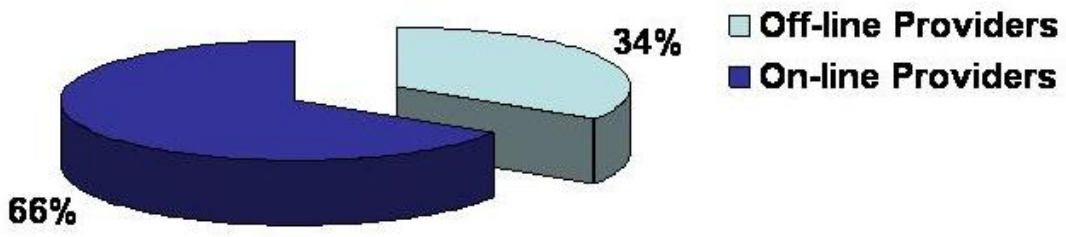

Figure 1: Types of PHR Providers

Figure 2 further describes how many of the thirty-three (33) researched on-line PHR providers shown in Figure 1 also offered some set of value-added services beyond the traditional health care journal services afforded through PHRs. Thirteen (13) of the thirty-three (33) researched on-line PHR providers, thirty-nine percent (39%), advertised

value-added services, where these services include interaction with a third party (e.g., secure communication with a care provider, prescription filling with a pharmacy, uploading of lab results data.)

Note: None of the researched off-line PHR providers advertised any value-added services.

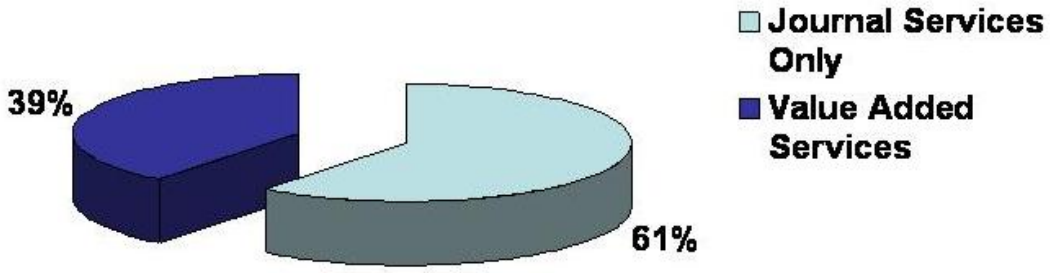

Figure 2: Services Offered by On-line PHR Providers

Of the thirteen (13) on-line PHR providers offering value-added services, Figure 3 shows the types of on-line services offered by these PHR providers, as well as how many of the on-line PHR providers offered each type of service.

Note: Some on-line PHR providers offered more than one value-added service, which is why the total number of providers shown in Figure 3 exceeds the thirteen on-line PHR providers offering value-added services.

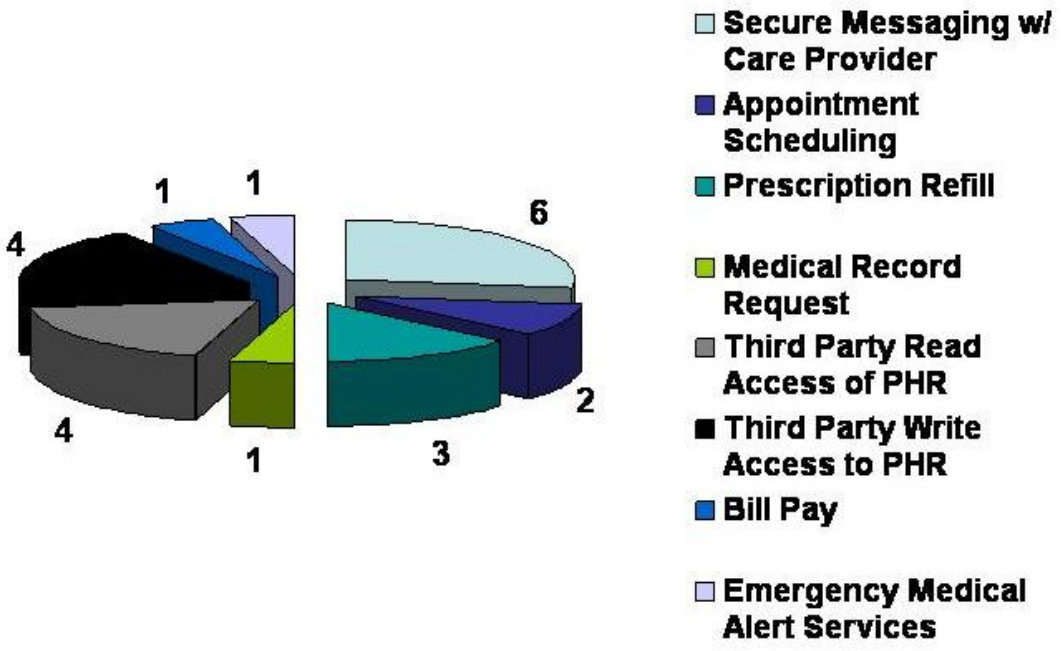

Figure 3: Valued-Added Services Provided by On-line PHR Providers

Each of the services in Figure 3 is further described below:

- *Secure Messaging with a Care Provider* – The health care consumer has the ability to securely consult (e.g., secure web messaging, secure e-ail) with a doctor or emergency medical staff to obtain medical information related to the consumer's PHR.
- *Appointment Scheduling* – The health care consumer has the ability to schedule an appointment with his/her doctor's office through an on-line calendar function offered by the PHR provider.
- *Prescription Refill* – The health care consumer has the ability to request an on-line refill with his/her doctor, and have the refill order placed with the consumer's pharmacy.
- *Medical Record Request* – The health care consumer has the ability to request a medical record from his/her care provider.
- *Third Party Read Access of PHR* – The health care consumer can identify who is authorized to view the PHR.
- *Third Party Write Access to PHR* – The health care consumer can identify who is authorized to write information into the PHR.
- *Bill Pay* – The health care consumer has the ability to directly pay a care provider health care bill on-line.

- *Emergency Medical Alert Services* – The health care consumer has the ability to provide emergency staff with access to their PHR information in emergency medical situations.

The remainder of this research will focus on the thirteen (13) on-line PHR providers offering value-added PHR services. Specifically, the following is addressed in the ensuing sections of this paper:

1) The identity proofing (IDP) practices implemented by the PHR providers prior to activating/establishing a PHR or PHR account for a consumer;
2) Examples of non-health care providers' IDP practices for identifying a consumer with no prior relationship;
3) Whether the provider web site published a privacy policy[1] that addressed how personal information was collected, managed, stored and transferred;
4) The type of identity authentication credential required to access a PHR or PHR account once consumer IDP was successfully completed;
5) Any miscellaneous items that made a particular provider appear to be more or less secure, in relation to the majority of the other providers researched.

[1] Identity proofing requires collection of personal identity data. Privacy policies play a role in disclosing a provider's practice for adequately protecting and managing personal identity data.

SUMMARY OF IDP PRACTICES

Of the thirteen (13) value-added PHR services providers researched and as shown in Figure 2, five (5) of the providers, thirty-eight percent (38%), offered no information as to how identity proofing was performed by the PHR provider prior to establishing and/or activating a PHR or PHR account. See Figure 4.

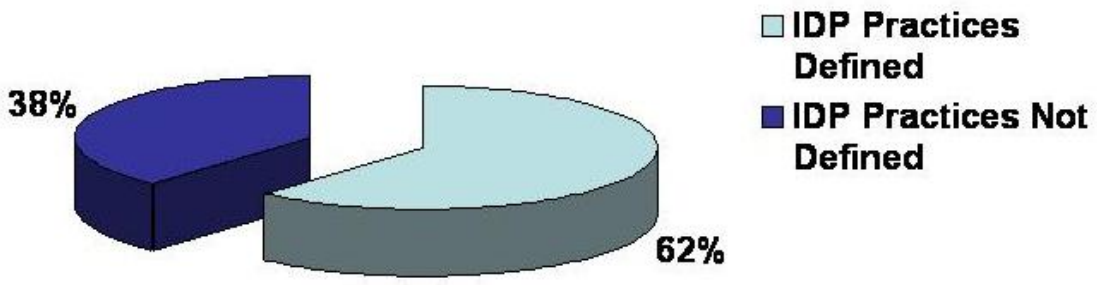

Figure 4: IDP Processes for Value-Added PHR Services

For those eight (8) providers that defined IDP processes, all of the providers required name and email address to be provided by the consumer (see Figure 5). The two (2) providers that only required name and email address offered free PHR services. In addition to name and email address:

- Three (3) PHR providers also required mailing address, phone number and credit card number to be verified.
- One (1) PHR provider also required mailing address, phone number, credit card number and age to be verified.
- One (1) PHR provider also required mailing address, phone number, social security number and date of birth to be verified.
- One (1) PHR provider also required mailing address, phone number, credit card number and an ID of the PHR device that was purchased by the consumer to be verified. (The Device ID was used by the PHR provider as part of the consumer identity proofing process to establish an on-line PHR service for the consumer.)

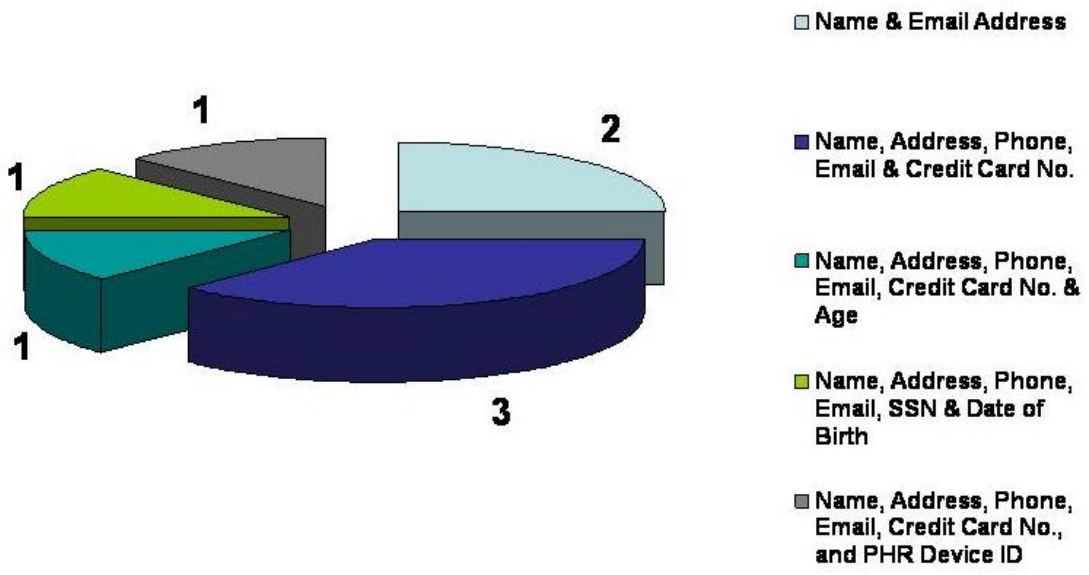

Figure 5: Identity Data Verified by PHR Providers Offering Value-Added Services

Table 1 further analyzes the IDP practices by mapping them to the specific value-added service shown in.

Value-added Service	**Name & Email Address**	**Name, Address, Phone, Email & Credit Card No.**	**Name, Address, Phone, Email, Credit Card No., & Age**	**Name, Address, Phone, Email, SSN & DoB**	**Name, Address, Phone, Email, Credit Card No., & PHR Device ID**
Secure Messaging w/ Care Provider	X	X		X	
Appointment Scheduling	*Information on identity proofing practices not found.*				
Prescription Refill	*Information on identity proofing practices not found.*				
Medical Record Request by Consumer	*Information on identity proofing practices not found.*				
3rd Party Read Access to PHR		X	X		X
3rd Party Write Access to PHR	X				
Consumer Bill Pay	*Information on identity proofing practices not found.*				
EMT Alert Services		X			

Table 1: Mapping of IDP Practices to Value-Added Services

In all cases researched above, identity proofing was performed by PHR providers to identity proof the health care consumer and no one else (including third parties who may be granted access to the PHR by the consumer). Once the health care consumer's identity had been established, the consumer was permitted to utilize value-added services defined by that PHR provider, assuming that third party relationships had been established by the health care consumer (i.e., each of the value-added services in Table 2 require interaction between the health care consumer and an authorized third party such as a caregiver or pharmacy). Unfortunately, there is little information available as to how the health care consumer identifies and authorizes third party access to PHRs and PHR information. Research suggests that PHR providers assist the health care consumer in establishing these third party relationships, or that both the consumer and the authorized third party agree to use the same PHR provider.

Research also shows that minimal health care consumer identity proofing is being performed prior to establishing a PHR that provides value-added services, where those services permit authorized third party access to PHRs. Four (4) of the value-added services (appointment scheduling with a doctor's office, prescription refill with a doctor and pharmacy, consumer medical record request, and consumer bill pay) had no mapping to IDP practices because those practices were not able to be determined by the PHR provider. For the remaining four (4) value-added services (secure messaging with a care provider, 3rd party read access to the PHR, 3rd party write access to the PHR, and emergency medical alert services), the identity proofing is largely based on a credit card transaction being successfully processed to purchase the PHR. In one (1) instance, write access to a PHR by a third party could be performed after only using name and email address to verify the consumer's identity. This was a significant finding that exhibits how low the assurance level is in trusting the identities of the health care consumer or authorized third parties accessing PHRs.

There is technology that exists today that could assist these PHR providers that have no prior relationship with a consumer. The technology is referred to as Knowledge Based Authentication (KBA), and it is offered by companies such as Experian[2], Equifax[3] and TransUnion.[4] Although the term "authentication" is used in the name of this technology, the technology is used to perform real-time identity proofing of a consumer prior to permitting the consumer to access information (e.g., personal information). KBA is based on algorithms developed by these companies, where those algorithms leverage aggregated information about a consumer to pose personal questions to the consumer in an attempt to identity proof the consumer. Those questions can relate to where the consumer has previously lived, previous and current mortgage payments, where the consumer went to school, etc. Additional information on KBA can be found at http://csrc.nist.gov/kba/.

[2] http://www.experian.com/
[3] http://www.equifax.com/
[4] http://www.transunion.com/

NON-HEATLHCARE IDP EXAMPLES

To provide information on how other industries are addressing the issue of consumer identity proofing where no prior relationship exists, the following three examples are provided:

- Obtaining a credit report from www.annualcreditreport.com
- Establishing an on-line money market account at www.capitalone.com
- Establishing an on-line savings account at www.hsbcdirect.com

Table 2 summarizes the identity verification information collected by each of these sites, the method used by the site to validate the identity information, the account activation method (if required), and the authentication credential delivered to the consumer upon successfully being identity proofed.

	Annual Credit Report	**Capital One**	**HSBC Direct**
Initial Set of Identity Information Collected	Legal Name SSN Date of Birth Mailing Address Residency More than 2 Years?	Legal Name Citizenship SSN Date of Birth Driver's License/State ID # Email Address Mailing Address Phone Number Residency More than 2 Years?	Legal Name Citizenship SSN Date of Birth Driver's License/State ID # Email Address Mailing Address Phone Number Residency More than 2 Years?
Additional Set of Identity Information Collected	Personal Questions* Mortgage provider? Mortgage amount? Car loan provider? Car loan amount?	Personal Questions* Car loan provider? Car loan term? Personal loan provider? Personal loan amount? Credit card provider?	Personal Questions* Student loan provider? Student loan amount? Car loan provider? Car loan amount? Credit card provider?
Method Used to Verify Identity Information	Third Party Source Verification and Knowledge Based Authentication	Third Party Source Verification and Knowledge Based Authentication	Third Party Source Verification and Knowledge Based Authentication
Account Activation Method	Immediate	Log back in with account information, SSN and email address to establish on-line account access; also required to provide 3 security answers for customer support.	Log back in with account information and SSN to establish on-line account access.
Authentication Credential	Credit report number provided by credit agency, along with State, Zip Code and SSN	Username/password	Username/password

Table 2: IDP Processes by Non-Health care Entities with No Prior Relationship with Consumer
* Personal questions are geared toward the applicant based on their verified credit information. Verified credit information is determined from the initial set of identity information collected from the applicant.

In each of the examples above, an initial set of identity information is collected by the service provider. This information is then verified using trusted third party sources (e.g., credit bureaus, state motor vehicle associations). Once the initial set of identity information is verified, credit information can be determined for the applicant. The credit information then drives a set of personal and financially related questions for the applicant to answer, using KBA technology. Upon successfully answering these questions, the applicant is successfully identity proofed by the service provider.

Compared to the research performed for the PHR providers, the IDP processes implemented by the credit reporting agencies supporting the www.annualcreditreport.com site, as well as by Capital One and HSBC Direct are more stringent than any of the IDP processes performed by the PHR providers. If one assumes that personal health care information is at least as sensitive as a consumer credit report, or the information contained within an on-line consumer banking account, then one can conclude that the PHR IDP processes need to be enhanced based on the research in this paper.

CONSIDERATIONS FOR THE CPS WORKING GROUP

Given the findings in this research paper, the following items are recommended to be considered for discussion within the CPS WG to develop recommendations for establishing remote electronic access to PHRs that provide adequate security and privacy for the PHR consumer:

- Should PHR providers offering value-added services be required to explicitly describe their identity proofing practices on their provider sites?
- Are technologies such as KBA, along with utilization of on-line trusted third party sources adequate to perform identity proofing of a PHR consumer where the consumer has no prior relationship with the PHR provider?
- Should third parties who have access to a PHR be identity proofed separately from the consumer? Further, should the identity proofing be more stringent for those third parties that have write access into a PHR?
- Should the degree of identity proofing be commensurate with the type of value-added services being provided by the PHR provider (e.g., is appointment scheduling less sensitive than communicating with a care provider, and therefore requires less identity proofing to be performed)?

APPENDICES

The information contained in the following appendices represents the thirteen (13) PHR providers offering value-added PHR services.

APPENDIX A – SUMMARY OF PRIVACY POLICIES

Privacy policies are included in this research as they represent a way for PHR providers to publish their IDP practices to patients, and assure patients that the identity data being collected from them is being used solely for the purpose of providing or establishing a PHR. In addition, privacy policies are used to assure the consumer that their personal information is being adequately protected and in accordance with applicable laws and regulations.

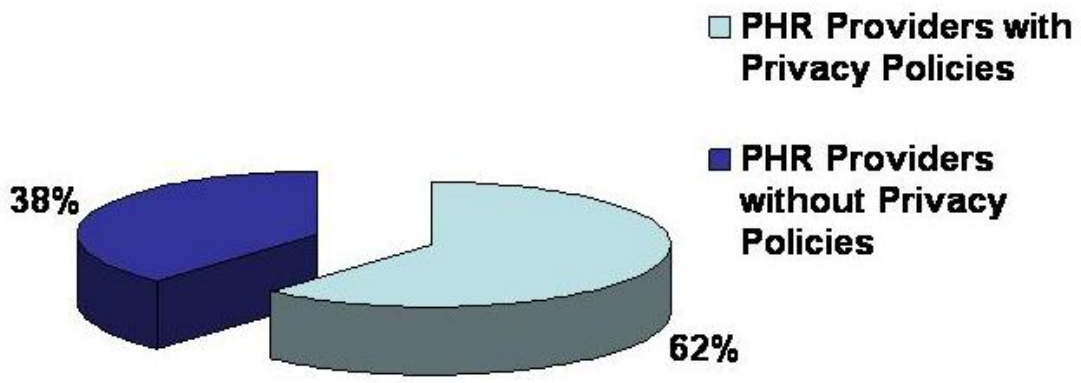

Figure 6: Valued-Added PHR Providers with a Published Privacy Policy

Eight (8) out of the thirteen (13) value-added PHR providers researched (62%) had an easily noticeable and accessible privacy policy on their web sites. These policies typically addressed why personal information was being collected, how it was used to manage the consumer's PHR account, the types of security and privacy measures employed by the provider, the rules around transferring information to business partners and 3rd parties, the use of cookies, and any other general information to assure the consumer that his/her personal health information was being securely managed. Of the 8 sites with privacy policies, only one (1) displayed the mark from Trust-e,[5] which certifies consistency with government and industry guidelines concerning the use of personal information. These standards include the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, the Federal Trade Commission and Department of Commerce's Fair Information Practices, the California Online Privacy Protection Act, and the CAN-SPAM Act.

[5] Information on Trust-e can be found at www.truste.org.

APPENDIX B – SUMMARY OF AUTHENTICATION CREDENTIALS

Authentication credentials are included in this research, as they represent the information that is provided to a consumer (upon successfully verifying the consumer's identity) to access the consumer's PHR or PHR account. Deficiencies in the authentication credentials or how the credentials are distributed to the consumer can result in security and privacy issues associated with the consumer's PHR (e.g., unauthorized access to medical information, identity fraud).

Figure 7 shows the authentication credentials implemented by the value-added PHR providers researched in this paper.

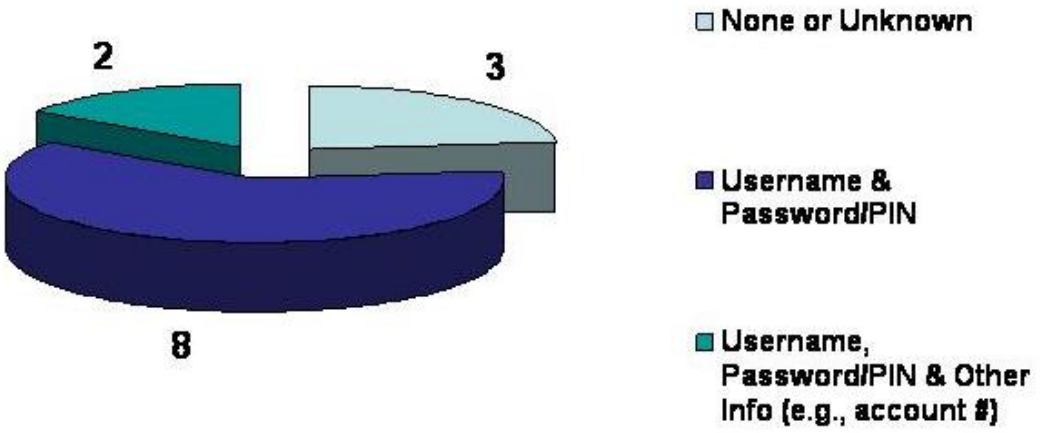

Figure 7: Types of Authentication Credentials Used by Value-Added PHR Providers

Username (or some form of a user ID) and password/PIN are the most implemented form of user authentication to PHRs, which is a form of single-factor authentication. However, three (3) of the providers researched did not provide any authentication information. Users could also provide their passwords/PINs to other authorized third parties (e.g., care providers) to allow these other third parties access to the patients' PHRs. In two (2) cases, users were required to provide an account number or unique ID along with their username and password/PIN. While additional information is being requested, it is still considered single-factor authentication of the user.

The financial community has long used username/password (a single-factor authentication mechanism) as the authentication credential for their on-line banking consumers. But in recent years, the Federal Financial Institutions Examination Council (FFIEC) has determined that,

> *"…single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties."*[6]

In response to the FFIEC guidance, financial institutions are now beginning to implement multi-factor authentication solutions for their on-line banking customers. Given the sensitivity of information that can exist in a PHR, and that nearly 1/5 of the PHR providers researched also allow a user to grant access to other authorized third parties to access the PHR, stronger authentication to a PHR may be required than what the research in this paper has uncovered.

[6] http://www.ffiec.gov/pdf/authentication_guidance.pdf

APPENDIX C – OTHER MISCELLANEOUS FINDINGS

When conducting this research, two (2) of the PHR provider sites (13% of all providers researched) had issues with their Secure Socket Layer (SSL) Site Certificates. These certificates are used to authenticate the PHR provider site as being a valid site. The certificates were found to 1) be expired, 2) not be trusted to a locally defined root authority in a common Internet browser, or 3) not contain a name in the certificate that matches the domain name of the provider web site.

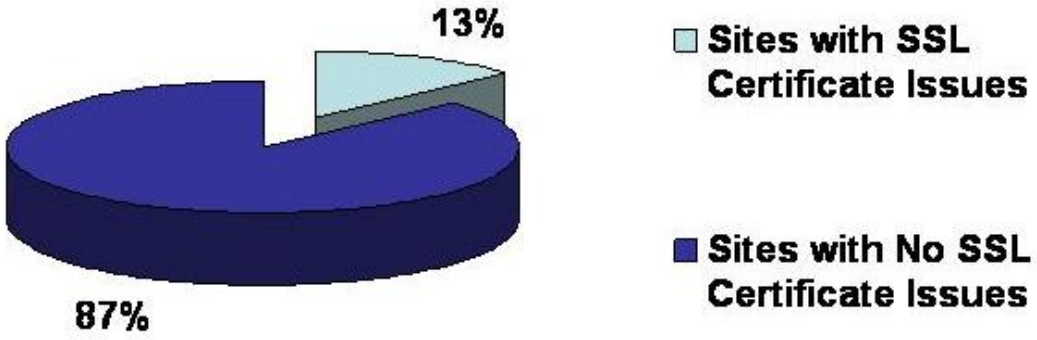

Figure 8: PHR Provider Web Sites with SSL Certificate Issues

In these instances, warning messages appear that alert users to question the trust of the SSL Site Certificate, and thus the trust of the PHR provider web site. Not trusting the SSL Site Certificate inhibits or limits secure access to the PHR provider web site, and may cause patients to have concern with the overall trust and security of the PHR provider site. For example, note the warning message that is displayed in the Internet Explorer 7 web browser when there is an issue with an SSL Site Certificate:

"There is a problem with this website's security certificate.

We recommend that you close this webpage and do not continue to this website."

An uneducated consumer may react very strongly to such a message and believe that his/her PHR information is not being adequately protected.