Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Using a Hybrid Technology Acceptance Model to Explore How Security Measures Affect the Adoption of Electronic Health Record Systems

Barbara Hewitt
Texas A&M Kingsville, barbara.hewitt@tamuk.edu

Using a Hybrid Technology Acceptance Model to Explore How Security Measures Affect the Adoption of Electronic Health Record Systems

Barbara Hewitt
Texas A&M Kingsville – San Antonio
Barbara.hewitt@tamuk.edu

ABSTRACT

While the adoption of computer systems is pervasive in most industries, few healthcare organizations have implemented electronic health record systems. Security is a major issue for these healthcare organizations. Security concerns include breaches of privacy and medical identity theft. This article uses a hybrid technology acceptance model (TAM) to explore why healthcare organizations are slow to adopt an EHR and slower to adopt biometric technology and single sign-on functionality despite the benefits of these systems. This paper advocates that healthcare organizations should adopt biometrics for authentication purposes, allow for multiple connections by each healthcare provider, and use single sign-on systems when implementing EHR systems. This research will also determine how costs, compliance issues, and security issues impact an individual's attitude when asked to use EHR systems.

Keywords (Required)

Electronic Health Records, Technology Acceptance Model, Innovation Diffusion Theory

INTRODUCTION

Computers are prevalent in most industries; however, healthcare organizations lag behind in this diffusion of technology. Lohr (2008) determined that just over 50% of large physician groups have adopted an electronic health record (EHR) system. DesRoches, Campbell, Rao, Donelan, Ferris, Jha, Kaushal, Levy, Rosenbaum, Shields, and Blumenthal (2008) found that only four percent of the 2758 physicians they surveyed had a fully functional electronic record system and 13% indicated that they had a basic computerized system.

The Standards for Privacy of Individually Identifiable Health Information (PIHI) section of the Health Insurance Portability and Accountability Act (HIPAA) mandates the regulation of privacy for individually identifiable health information (Congress, 1996, 2001, Gunter and Terry, 2005). President Bush issued Executive Order 13335 that mandated healthcare organizations implement EHR for most Americans by 2014 (Horowitz, Mon, Bernstein, and Bell, 2008).

Although many physicians and healthcare organizations indicate that potential costs associated with the adoption of electronic records preclude them from purchasing systems (DesRoches et al., 2008, Thakkar and Davis, 2006), HR. 1 that provides the National Institute of Health with $19 billion for the development and use of electronic health records (Congress, 2009, Huslin, 2009). Healthcare organizations will see improved efficiency. EHR systems enable providers to manage chronic disease more effectively and reduce orders for duplicate tests and procedures (Hammond, 2004). The potential savings of effective EHR implementations at $81 billion annually (Hillestad, Bieglow, Bower, Girosi, Melli, Scoville, and Taylor, 2005).

Healthcare organizations identify many different issues when deciding whether to adopt an EHR system. This research will explore whether security measures such as biometrics authentication, multiple access systems, and single sign-on systems will increase the likelihood of EHR adoption. This research will also determine whether costs, compliance issues, and security issues hinder the adoption of EHR systems.

LITERATURE REVIEW

Healthcare organization must address many issues when adopting an EHR system. First, they must ensure patient confidentiality and privacy (Runy, 2008). This concern extends beyond privacy issues to other security concerns when organizations adopt EHR systems (Hillestad et al., 2005). Breaches of patient confidentiality occur daily regardless of whether the compromise is the result of an accidental disclosure or a deliberate violation of the patient's privacy and confidentiality. Healthcare providers must view patient records on a "need to know" basis (Myers, Frieden, Bherwani, and Henning, 2008, Runy, 2008). Breaches include attaching documents that contain confidential patient information to email messages, having laptops with confidential information stolen, and accessing healthcare records of celebrities, acquaintances, friends, and colleagues.

An emerging concern for healthcare organizations is medical identify theft (Andrews, 2008) which occurs when a person without medical insurance assumes the identity of an insured individual to receive medical services such as surgery or drugs (Andrews, 2008). In this type of identity theft, the uninsured's medical information is often incorporated into or replaces the insured's medical record causing major medical issues and risk to the rightful owner of the medical record. Medical identity theft also occurs when a healthcare provider files fraudulent healthcare claims to be reimbursed for procedures that were not performed on a patient and bilks Medicare, Medicaid, and insurance companies out of millions dollars (Andrews, 2008).

Accessibility is another issue that must be addressed by healthcare providers. Healthcare providers must access multiple systems including radiology, pharmacy, clinical, and surgical systems when caring for a patient. When a provider must sign onto each system individually, access to the information is not instantaneous and the patient's health could be compromised in crucial emergency situations.

While some healthcare facilities have a computer or handheld device available for each staff member's and physician's use, other facilities may require that healthcare providers share computers either within a patient's room or at the nurse's station. Each individual must authenticate each time they access patient information at a different workstation. When the healthcare provider returns to the computer to view patient information after a while, the system has locked and they must re-authenticate and log onto multiple different systems again.

Healthcare environments are dynamic and disruptive. When healthcare providers are faced with crises that require immediate attention, these crises often cause the provider to quickly leave a workstation unattended. In order to maintain security, computer systems must have a short time-out setting. During the crisis, the provider may need to access patient information to view information that could be life saving. However, the time required to re-authenticate may be life threatening to a patient.

Healthcare organizations use different mechanisms for authentication including passwords, smart cards, digital signatures, and biometrics (Andrews, 2006, Krawczyk and Jain, 2005). Passwords are often used as the first line of defense of a patient's confidential information (Medlin and Romaniello, 2007); however, Duke found that over 40% of the calls to the IT helpdesk occurred when healthcare providers forgot their passwords and could not log onto the system (Ashmad and Rodriquez, 2006). While passwords suffice in many organizations, calling upon the helpdesk to reset a forgotten password can compromise a patient's life. Password strength is often compromised so that the user can remember the password. In a study on password strength, Medlin and Romanelli (2007) used a password cracking program to study password strength of 90 healthcare workers. Over 31% of the passwords were cracked in less than a minute and over 50% within the first hour.

Consequently other measures should be used for authentication. Smartcards can be used in lieu of passwords; however, smartcards can be lost, stolen, copied, or damaged. The requirement that the person be physically present to authenticate using devices such as biometric devices increases the chances of proper authentication.

Some healthcare organizations that have adopted EHR systems also implemented some form of biometrics. Healthcare organizations are the largest user groups of Sentillion's fingerprint biometric technology (Andrews, 2006). Other healthcare providers are using handprint scanners, retinal scanners, face geometry scanners, an dynamic signatures (Andrews, 2006). Vincent's Hospital and Healthcare Center, a network of eight hospitals and ancillary healthcare facilities in the Indianapolis area, are using fingerprint scanners (IndentiPHI, 2007).

Healthcare organizations face many challenges when implementing biometric devices in a healthcare setting. For example touch type devices such as fingerprint and palm scanning devices are sensitive to dirt, grime, grease, and cleaning solutions (IndentiPHI, 2007, Scott, 2004). Healthcare environments must be kept sterile. Providers often wear gloves which may also

hinder the practicality of touch type device. Non-touch devices such as facial scanners, retinal scanners, and voice recognition devices are less intrusive. While these devices do not require physical contact, surgical healthcare providers often cover their faces with masks or shields posing issues that may interfere with some of these devices. Voice pattern recognition may be more applicable in these environments. Krawczyk and Jain (2005) determined that digital signatures (private key authentication) and voice modalities biometrics are robust authentication methods for physicians using tablet PCs. Thus a multitude of biometric systems should be explored and incorporated into these systems.

Healthcare organizations must overcome issues related to accessing multiple systems (e.g., radiation, physical therapy, pharmacy) simultaneously. Often these systems are not interconnected and users must authenticate on each system using different usernames and passwords. A solution to the multiple system access issue would be a single sign-on (SSO) system. Individuals using a SSO system would be able to gain access multiple systems simultaneously.

The adoption of an EHR does not guarantee that the healthcare organization will also espouse a SSO and/or a biometric device. However, healthcare providers may be more reticent to adopting EHR when the system has an easy authentication method that allows the provider quick access to vital information about the patient for whom he/she is administering care. Duke University Medical Center and Health System have SSO systems for their most critical applications. St Vincent's Hospital and Healthcare Center One successfully implemented both biometrics and SSO access with their EHR system (IndentiPHI, 2007). The best solution would be an EHR that encompasses a single sign-on system, that easily handles multiple users per station, and that uses biometrics for authentication.

PROPOSED MODEL

Davis's (1989) explored the adoption of technology using the technology acceptance model (TAM). TAM used factors, perceived usefulness and perceived ease of use, to examine what influences an individual's intention to use a specific technology (Davis, 1989).

Roger's (1995) innovation diffusion theory (IDT) investigates how users integrate a technology into their environment by exploring how diffusion is influenced by social systems, innovation, communication channels, and interaction over time (Rogers, 1983). The factors that are often used to explore innovation of IDT include observability, trialability, compatibility, complexity, and relative advantage. Factors that influence social systems include task, individual, organization and environment. Kwon and Zmud (1987) proposed that adoption is influenced by incorporating task and environmental factors with those of Rogers.

Wu and Wu (2005) integrated aspects of TAM with IDT to explore the adoption of customer relationship systems. Wu and Wu indicated that Perceived Ease of Use as used in TAM is similar to Complexity construct in IDT. Perceived Usefulness as found in TAM is comparable to Relative Advantage of the IDT model. Wu and Wu's proposed model is shown in Figure 1.

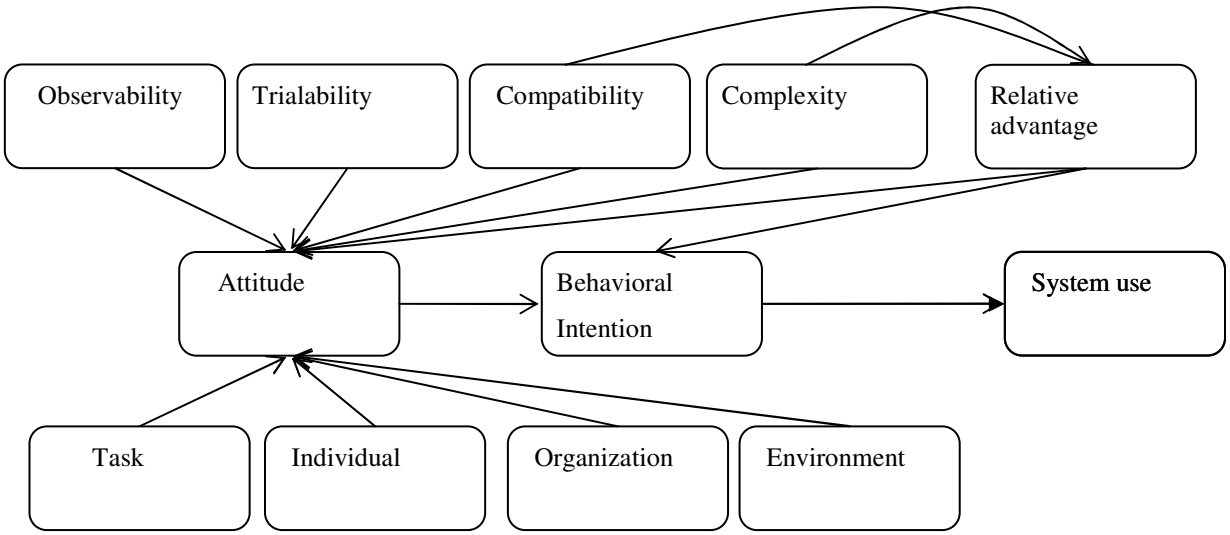

Figure 1. Wu and Wu (2005) Hybrid Technology Acceptance Model

The model proposed for this research incorporates factors that influence the decision to adopt an EHR with Wu and Wu's (2005) hybrid TAM. As stated previously, physicians and health care organizations choose costs as the biggest obstacle to EHR adoption. HR. 1 sets aside over $19 billion towards electronic health records (Congress, 2009). Security is a huge issue for healthcare practitioners. Healthcare records must be kept secure in order to maintain patient confidentiality. Therefore, cost, compliance issues, and security will be incorporated into the Wu and Wu's (2005) Hybrid TAM model.

Healthcare providers must access the information within patient's healthcare records in order to treat the patient. This access must be easily granted regardless of whether they are in the emergency room, a patient's room, at a nurse's station, or at home. They are concerned with the ease of use and the usefulness of an EHR system. Biometric devices, multiple access systems, and single sign-on systems will increase the ease of use of an EHR. The proposed model is shown in Figure 2. The patient's privacy must be upheld. Identity theft must be minimized. An EHR with proper authentication software can assist in solving some of these issues Biometrics can be used to augment the authentication method. A single sign-on system would eliminate the need to remember multiple passwords for each different clinical system a healthcare provider is attempting to access.

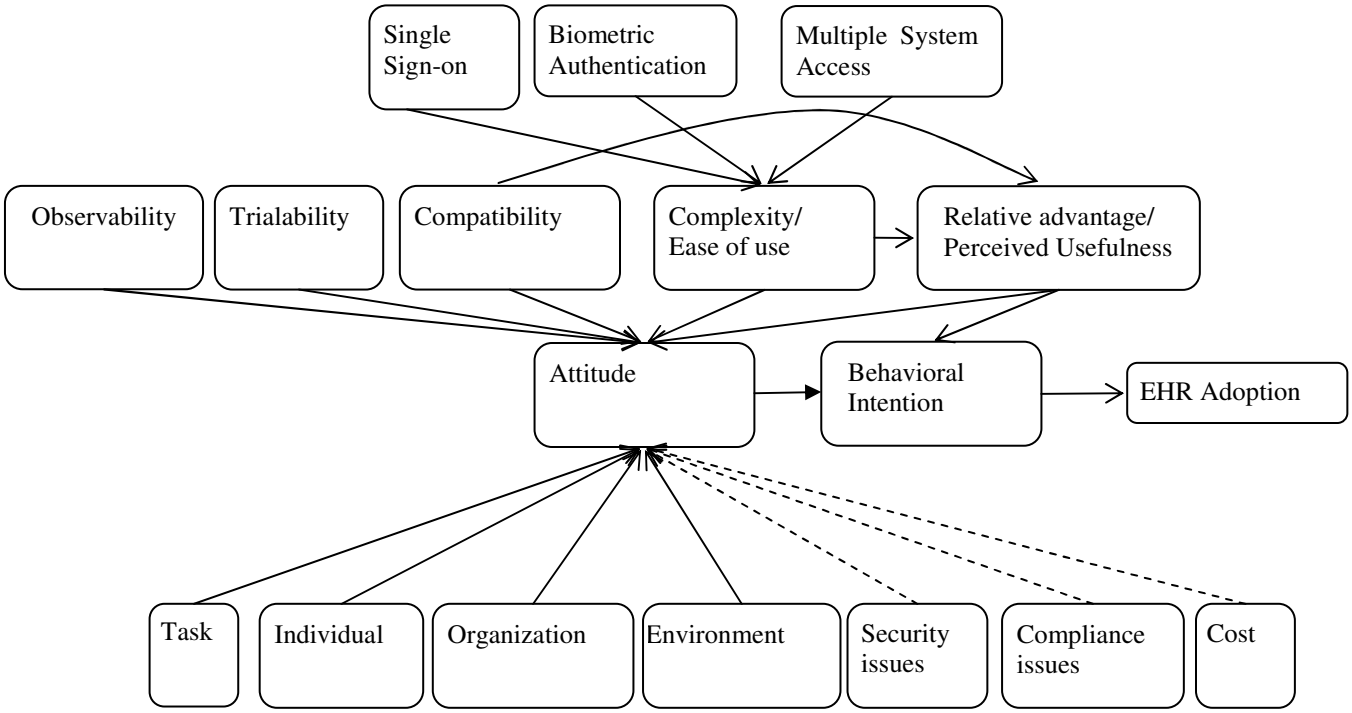

Figure 2. Proposed EHR Adoption Model

Observability indicates to what extent others are able to observe the innovation (Moore and Benbasat, 1991). When an EHR is implemented in an organization, most individuals will observe others using the software. Observability should have a positive effect on an individual's attitude toward using the EHR. Trialability is the ability to experiment with the technology prior to adoption (Moore and Benbasat, 1991). Individuals are able to try the technology such as they would during training sessions prior to adoption of the EHR. Their attitude for the EHR should be positively impacted by trialability. Compatibility refers to the perception that the technology is "consistent with the existing values, needs, and past experiences of potential adopters" (Moore and Benbasat, 1991, p. 195). Healthcare providers should find the EHR compatible with their goal to provide good patient care. Thus compatibility should positively affect the individual's attitude toward EHRs.

Complexity is the degree that an innovation is seen as difficult to use. Complexity from Davis' IDT model is completely opposite of Davis' ease of use variable. Biometric authentication devices, single sign-on systems, and multiple use systems should make an EHR easier to use. Thus this research expects that these items will increase the use's perception that the EHR is easier to use. A user's attitude toward an EHR will be positively impacted by its ease of use.

Relative advantage/usefulness is defined as "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989, p. 230). While some believe that EHRs are useful, others disagree. Haug

(2009) discusses how while some view EHRs as useful, others find EHRS useless. For example, physicians found that computerized physician order entry (CPOE) systems were harder to use than expected (Haug, 2009). They also could not make non-generic notations or add simple drawings to these systems (Haug, 2009). This research predicts that healthcare providers will believe that EHRs are useful. If individuals feel the system is useful, usefulness will have a positive impact on their attitude toward EHR systems and their intention to use EHR systems.

Task is measured using task structure, the autonomy of the task and the uncertainty of the task (Kwon and Zmud, 1987). These task characteristics will negatively impact the user's attitude toward an EHR system. Individual that influence task adoption would include age, education, experience and personal traits (Wu and Wu, 2005). While some may argue that EHR systems are mandatory for staff members, almost 19% of organizations surveyed by the Medical Records Institute removed EHR systems (Conn, 2007). Thirty percent of the respondents indicated that clinicians are refusing to use their EMR with over 12% of these systems being removed due to lack of clinician usage (Conn, 2007). Thus individual factors will have an effect on the attitude about EHR systems.

Organizational factors include top management support, organizational size, user involvement, and product champion (Wu and Wu, 2005). Organizational factors will have an impact on EHR systems. Environmental factors include competitor pressure, customer satisfaction, and marketing approach (Wu and Wu, 2005).

Other factors that have been identified in past research to inhibit the adoption of EHR systems include costs, security issues, and compliance issues. Cost was the major issue identified by both hospitals and individual physicians as impeding the implementation of EHRs. Security of an EHR system is a major issue with either paper-based or electronic records. With Obama backed Bush's Executive order 13335, healthcare organizations are still expected to adopt EHR systems by 2014. These issues will all have an impact on the individual's attitude toward EHRs.

METHODOLOGY

The model will be tested using a field survey. The survey instrument is Appendix A. The items in the survey were adapted from previous studies. Items developed by Moore and Benbasat (1991) will be used to measure IDT factors including innovation, relative advantage, compatibility, complexity, observability, and trialability. The survey will include Kwon and Zmud's (1987) measure for task, individual, organizational, and environmental factors. The items to measure attitude will be constructed using advice from Azjen and Fishbein (1980). Behavioral intention and usage items will be adapted from Davis (1989). The items to measure security issues, compliance issues and cost will be added based on questions found in the other surveys.

To test reliability and validity, a pilot study is being administered to employees in all areas of Southwest General Hospital in San Antonio, Texas[1]. While the individuals at this facility are mandated to use the hospital's system, they should still be a good proxy for other healthcare providers. The EHR system at the hospital was installed in 2005.

This study used SmartPLS (Ringle, Wende, and Will, 2005) to perform partial least squares (PLS) analysis (a structure equation modeling techniques) on the pilot study data (Gefen and Straub, 2005). PLS analysis is often used in information systems research studies to analyze survey data (Chin, 1998a, Chin, Marcolin, and Newsted, 2003, Gefen and Straub, 2005, Gefen, Straub, and Boudreau, 2000). This research used PLS since it analyzes data with smaller sample sizes with few stipulations for underlying data distribution (Chin, 1998b).

Table 1 shows the Average AVE, ρ_c, and CA for the latent variables. Yi and Davis (2003) prescribe that the composite reliability is greater than .07. Using the current pilot study data, many items fall below this minimal threshold. Again these results are inconclusive since the pilot study is currently underway.

[1] Special thanks to Southwest General Hospital, San Antonio, Texas who agreed to participate in this study and to have their name included in the paper.

	AVE	Composite Reliability ρ_c	R^2	Cronbach Alpha
Attitude	0.6744	0.9484	0.8754	0.9371
Behavioral Intention	0.6805	0.8098	0.4336	0.5311
Biometric Authentication	0.7105	0.9068	0	0.8672
Compatibility	0.7612	0.9271	0	0.8950
Compliance	0.4970	0.7411	0	0.4818
Cost	0.6527	0.9240	0.3032	0.8953
Complexity/Ease Of Use	0.4062	0.6390	0	0.3863
Environmental	0.6941	0.8702	0	0.7967
Individual	0.7337	0.8920	0	0.8212
Multiple Sign-on Access	0.8449	0.9645	0.6004	0.9537
Observability	0.8253	0.9659	0.7926	0.9573
Organization	0.3864	0.0236	0	0.3923
Single-sign On	0.5327	0.7726	0	0.5918
Security Issues	0.4868	0.7778	0	0.6841
Task	0.7120	0.8298	0	0.6288
Trialability	0.2801	0.4477	0	0.4890
Use	0.5567	0.7857	0	0.6815
Relative Advantage/ Usefulness	0.5437	0.7244	0	0.4791

Table 1 - AVE, ρ_c, and Cronbach Alpha

The factor loadings are shown in Table 3 in Appendix B. If the factor loadings are still inconclusive after the pilot study is completed, then the original survey must be modified based on these results and a second pilot study administered. Once the survey is reliable and valid, the researcher will survey healthcare providers to determine what influences their use of EHRs. The survey will be offered online or via a paper document. Paper-based and online surveys offer similar results and can be used interchangeably (Carini, Hayek, Kuh, Kennedy, and Ouimet, 2003).

Gefen, Straub, and Boudreau (2000) recommend that researchers should use path analysis to analyze multiple paths of a model simultaneously since conventional statistical analysis procedures such as ANOVA, linear regression, multiple regression analysis, and factorial analysis only test the individual paths. This study will use SmartPLS, a partial least square (PLS) to test the model.

PRELIMINARY RESULTS

A total of 61 individuals completed the survey; however, 3 surveys were incomplete and removed from the analysis. The preliminary results for the 58 individuals who responded to the pilot study thus far are shown in this section. The pilot study is ongoing so results may change as more data is collected. Table 2 shows the results of PLS analysis.

	Original Sample	Sample Mean	Standard Deviation	Standard Error	T Statistics	P-value
Attitude -> Behavior Intent	0.0232	0.0143	0.1686	0.1686	0.1379	0.4454
Behavior Intent -> Use	0.7749	0.7791	0.0456	0.0456	17.0088	0.0000
Biometric Authentication -> Ease Of Use	0.2076	0.2202	0.1668	0.1668	1.2450	0.1091
Compatibility → Attitude	0.1060	0.1087	0.1692	0.1692	0.6266	0.2667
Compatibility → Usefulness	0.7346	0.7070	0.1564	0.1564	4.6983	0.0000
Compliance → Attitude	0.0595	0.0699	0.1021	0.1021	0.5827	0.2812

Cost → Attitude	0.0768	0.0725	0.1627	0.1627	0.4723	0.3193
Ease Of Use → Attitude	0.1864	0.2123	0.1602	0.1602	1.1636	0.1247
Ease Of Use → Usefulness	0.2858	0.2744	0.1770	0.1770	1.6145	0.0560
Environment → Attitude	-0.1427	-0.1207	0.0934	0.0934	1.5275	0.0661
Individual → Attitude	0.1300	0.0897	0.1133	0.1133	1.1469	0.1281
Multiple Sign-on Access → Ease Of Use	0.1109	0.1407	0.1903	0.1903	0.5829	0.2811
Observability → Attitude	0.6397	0.6564	0.1878	0.1878	3.4058	0.0006
Organization →Attitude	-0.2348	-0.1879	0.1410	0.1410	1.6652	0.0507
Single Sign On → Ease Of Use	0.0066	0.0239	0.0940	0.0940	0.0704	0.4721
Security Issues →Attitude	0.4462	0.4596	0.1632	0.1632	2.7341	0.0042
Task → Attitude	-0.0365	-0.0565	0.1162	0.1162	0.3146	0.3771
Trialability → Attitude	0.0230	-0.0125	0.1048	0.1048	0.2193	0.4136
Usefulness →Attitude	0.0037	0.0479	0.1539	0.1539	0.0242	0.4904
Usefulness -> Behavioral Intent	0.2797	0.2663	0.1512	0.1512	1.8500	0.0347

Table 2 – PLS Analysis Results

CONCLUSION

Healthcare organizations are slow to adopt EHR systems despite the many benefits of using these systems and in spite of the need to address the Executive Order 13335. Costs and usability were the biggest concerns identified by healthcare organizations and physicians in adopting healthcare systems by previous research; however, costs were not found significant in the current study. Usefulness and ease of use both significantly affected behavioral intent which in turn impacted usage.

There are also issues that must be addressed. Accessibility issues should be a major concern of these organizations; however, these individuals did not think that biometric authentication, multiple sign-on access, or the single sign-on system significantly impacted the ease of use. Notably the facility used in the pilot study did not have either feature in place. Healthcare providers need immediate access to patient records as well as all other electronically stored and paper based information about a patient. The system should allow multiple users to access a single computer simultaneously; however, access should be limited so that each individual user can only access the information that he or she is authorized to view.

Limitations

This section addresses the limitations of this study. For example, some states have laws that prohibit the use of SSO systems. Some states may have laws that forbid or regulate the use of SSO systems. This study does not address the legal aspects or ramifications of using SSO systems or biometrics in a healthcare setting.
Due to the many factors being explored in this study, the survey will be long. The time required to complete the survey may hinder the response rate.

Theoretical Implications

This research will add to the theoretical exploration of the TAM model by exploring the adoption of biometrics and SSO in a healthcare setting. Past research into adoptions models have not included additional factors such as cost, security, and compliance which may be an issue in some environments such as healthcare.

Practical Implications

This study will offer healthcare organizations, software development firms, and the governing bodies what issues healthcare organizations are facing while adopting EHR systems. As prescribed above, healthcare organizations must adopt EHR systems by the 2014. It is imperative to get individuals within these organizations to use these systems. This research will provide insight into what issues are impeding the adoption of EHR systems. With a better understanding of the issues, organizations will be able to address some of the issues that impact the adoption EHR systems. Software firms and healthcare

organizations will know whether including different features such as biometric authentication, single sign-on, and multiple-access features will increase the likelihood that individuals will use these systems.

REFERENCES

1. Ajzen, I. and Fishbein, M. (1980) *Understanding Attitudes and Predicting Social Behavior,* Prentice-Hall, Englewood Cliffs, NJ.
2. Andrews, J. (2006) Biometrics leaves imprint on healthcare, *Healthcare IT News,* May 01.
3. Andrews, M. (2008) Medical identity theft turns patients into victims, *US News,* February 29.
4. Ashmad, A. and Rodriquez, R. (2006) Best Practices: Duke identifies with security needs, *Information Week,* October 1.
5. Carini, R. M., Hayek, J. C., Kuh, G. D., Kennedy, J. M., and Ouimet, J. A. (2003) College student responses to web and paper surveys: Does mode matter?, *Research in Higher Education,* Febuary **44,** 1,19.
6. Chin, W. W. (1998a) Issues and Opinion on Structural Equation Modeling, *Management Information Systems Quarterly,* **22,** 1,7-16.
7. Chin, W. W. (1998b) The partial least squares approach to structural equation modeling, *Modern Methods for Business Research,* **295**336.
8. Chin, W. W., Marcolin, B. L., and Newsted, P. R. (2003) A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study, *Information Systems Research,* **14,** 2,189-217.
9. Congress (1996) Health Insurance Portability and Accountability Act of 1996 (HIPAA), *Pub.L. 104-191, Aug. 21, 1996, 110 Stat. 1936*.
10. Congress (2001) Standards for Privacy of Individually Identifiable Health Information (PIHI), April 14,**codified at 45 CFR §160, §164**.
11. Congress, G. u. H. R.-.-t. (2009) American Recovery and Reinvestment Act of 2009, *GovTrack.us (database of federal legislation)*

Mar 31, 2009.

12. Conn, J. (2007) Failure, de-installation of EHRs abound; study. In: *ModernHealthcare.com*, pp.
13. Davis, F. D. (1989) Perceived usefulness, perceived ease of use, and end user acceptance of information technology, *MIS Quarterly,* **13**318-339.
14. DesRoches, C., Campbell, E., G, Rao , S. R., Donelan, K., Ferris, T. G., Jha, A., Kaushal, R., Levy, D., Rosenbaum, S., Shields, A., and Blumenthal, D. (2008) Electronic health records in ambulatory care -- A national survey of physicians, *The New England Journal of Medicine,* July 3,**359,** 1,51-60.
15. Gefen, D. and Straub, D. (2005) A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example, *Communications of the Association for Information Systems,* **16**91-109.
16. Gefen, D., Straub, D., and Boudreau, M. (2000) Structural Equation Modeling and Regression: Guidelines for Research Practice, *Structural Equation Modeling,* **4**.
17. Gefen, D., Straub Jr., D. W., and Boudreau, M.-C. (2000) Structural Equation Modeling and Regression: Guidelines for Research Practice, *Communications of the Association of Information Systems,* October,**4,** 7,1-77.
18. Gunter, T. D. and Terry, N. P. (2005) The emergence of national electronic health record architectures in the United States and Australia: Models, Costs, and Questions, *Journal of Medical Internet Research,* March 5,**7,** 1.
19. Hammond, W. E. (2004) Electronic medical records -- Getting it right and going to scale. In: *The Commonwealth Fund/ Nuffeld Trust Conference*, pp. 14. The Commonweatlh Fund, Pennyhill Park, Bagshot, England.
20. Haug, S. (2009) Electronic Medical Records: Will they really cut costs?, *Time* March 05,4.
21. Hillestad, R., Bieglow, J., Bower, A., Girosi, F., Melli, R., Scoville, R., and Taylor, R. (2005) Can electronic medical record systems transform health care? Potential health benefits, savings, and costs, *Health Affairs,* **24,** 5,1103-1117.
22. Horowitz, J., Mon, D., Bernstein, B., and Bell, K. (2008) Defining key health information technology terms. (Ed, Services, D. o. H. H.), pp. Office of the National Coordinator for Health Information Technology.
23. Huslin, A. (2009) Online Health Data in Remission, *The Washington Post,* Monday, February 16,**,** D01.
24. IndentiPHI, I. (2007) Biometric security for St. Vincent Hospital and Healthcare Centers. Vol. 2008, pp. IdentiPHI, Inc., Indianapolis.
25. Krawczyk, S. and Jain, A. K. (2005) Securing electronic medical records using biometric authentication. In: *Lector Notes in Computer Science*, Vol. 3546/2005, pp. 1110-1119. Springer Berlin, Berlin.
26. Kwon, T. H. and Zmud, R. (Eds.) (1987) *Unifying the fragmented models of information systems implementation,* John Wiley & Sons, New York.
27. Lohr, S. (2008) Most doctors aren't using electronic health records, *New York Times,* June 19,

28. Medlin, B. D. and Romaniello, A. (2007) An investigative study: Health care workers as security threat suppliers, *Journal of Information Privacy & Security* **3,** 1,17.
29. Moore, G. C. and Benbasat, I. (1991) Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation, *Information Systems Research,* September 1991,**2,** 3,192-222.
30. Myers, J., Frieden, T. R., Bherwani, K. M., and Henning, K. J. (2008) Ethics in public health research: Privacy and public health at risk: Public health confidentiality in the digital age, *American Journal of Public Health* **98,** 5,793-801.
31. Ringle, C. M., Wende, S., and Will, S. (2005) SmartPLS 2.0 (M3) Beta. pp. http://www.smartpls.de, Hamburg.
32. Rogers, E. M. (1983) *Diffusion of Innovations,* The Free Press, New York.
33. Rogers, E. M. (1995) *Diffusion of Innovation Theory,* Free Press, New York.
34. Runy, L. A. (2008) The best line of defense: Hospitals take a proactive approach to data security threats, *Hospitals and Health Networks,* Summer,**7,** 3,22-26.
35. Scott, M. (2004) Fingers point toward biometrics, *For the Record,* August 9,**16,** 16,29.
36. Thakkar, M. and Davis, D. C. (2006) Risks, barriers, benefits of EHR systems: A comparative study based on size of hospital, *Perspectives in Health Information Management,* August 14**,** 5.
37. Wu, I.-L. and Wu, K.-W. (2005) A hybrid technology acceptance approach for exploring e-CRM adoption in organizations, *Behaviour & Information Technology,* July,**24,** 4,303-316.
38. Yi, M. Y. and Davis, F. D. (2003) Developing and Validating an Observational Learning Model of Computer Software Training and Skill Acquisition, *Information Systems Research,* **14,** 2,146-169.

APPENDIX A: SURVEY

Computer Expertise

1. I am an expert on the topic of EHR
2. Overall, I consider myself a novice with respect to an EHR
3. I am very informed about EHR systems?

Relative Advantage/Perceived Usefulness

1. Using an EHR enables me to accomplish task more quickly
2. Using an EHR improves the quality of work I do
3. Using an EHR makes it easier to do my job
4. Using an EHR gives me greater control over my work.
5. The disadvantage of using an EHR far outweigh the advantages.
6. Overall, I find using an EHR to be advantageous in treating patients.
7. Using an EHR will improve my job performance.
8. Using an EHR enhances my effectiveness on the job.
9. Using an EHR increases my productivity.

Complexity/Ease of Use

1. My interaction with EHR is clear and understandable
2. I believe that it isn't easy to get the EHR to do what I want it to do.
3. Learning to operate the EHR is easy for me.
4. Learning to operate an EHR would be easy for me.
5. I would find it easy to get the EHR to do what I want it to do.
6. It would be easy for me to become skillful at using an EHR
7. Overall, I would find an EHR easy to use

Compatibility

1. Using the EHR is compatible with all aspects of my work.
2. Using the EHR fits into my work style.
3. I think that using the EHR fits well with the way I like to work.
4. Using an EHR is completely compatible with my current situation.

Observability

1. In my organization, one sees an EHR on many desks.
2. It is easy for me to observe others using an EHR in my facility.
3. I have had a lot of opportunity to see an EHR being used.
4. In my organizations, one sees others using the EHR./

Trialability

1. I have had a great deal of opportunity to try various EHR applications.

2. I know where I can go to satisfactorily try out various uses of an EHR.
3. My organization has sites available for me to try the various features of an EHR.

Task

1. The best practice of the task in the day-to-day activities are likely to be influenced by adopting an EHR.
2. Using the EHR will affect the independence of day-to-day activities.
3. I hesitant in using the EHR because it will affect the day-to-day activities.

Individual

1. Using an EHR is dependent on their education of relevant systems.
2. Using an EHR is dependent on the age of the individual.
3. Using an EHR is dependent on their experience with relevant IS applications.
4. Using IS innovations is dependent on the personal traits of the individual.

Organization

1. The greater the support from top management, the more likely an EHR will be adopted.
2. The size of the organization will affect an EHR adoption.
3. Using an EHR affects the patient's view of the facility's operations.
4. Using an EHR will require user involvement in the development process.
5. Using an EHR is based on the entrepreneur nature of the organization.

Environment

1. The pressure from competitors is likely to influence the decision to use an EHR.
2. The availability of external support for implementing an EHR is important to the success of using the innovation.
3. Using an EHR will positively affect the relationship we have with our patients

Biometrics - Security

1. Using biometric authentication will make the system more secure.
2. Using biometric authentication will increase the security of the EHR.
3. The EMR will be more secure if it uses biometric devices for secure authentication instead of a password.
4. Using biometric authentication will improve the security of the EHR

Security

1. I worry about security when using an EHR.
2. An EHR is a secure way to capture patient information.
3. Security is a concern when obtaining patient information using an EHR.
4. I am concerned about using an EHR due to security issues.

Compliance

1. There are government regulations that will require that we use an EHR system.
2. I am (will be) required to use an EHR due to government regulations.
3. In order for our facility to be in compliance with government regulations, I am using (will use) an EHR.
4. I am not aware of any government regulations that will require that I use an EHR.

Cost

1. EHR systems are very expensive.
2. My organization has not purchased an EHR because EHR systems are expensive.
3. The benefits of an EHR are higher than the costs of an EHR.
4. The EHR system is very expensive.

Biometric Devices

1. Biometric devices such as finger print scanners, retina scanners, face recognition devices will make it easier to use an EHR.
2. Using a biometric device such as finger print scanners, retina scanners, face recognition devices to authenticate on a EHR system will make the system easy to use.
3. It will be easier to use an EHR if I do not have to remember a password.
4. Biometric devices such as finger print scanners, retina scanners, face recognition devices will be easy to use for accessing an EHR.

Single Sign-On Systems

1. A single sign-on system will be easy to use.
2. A single sign-on system will allow me to use the system easily.
3. A single sign-on system will allow me to access more information about a patient making the EHR easier to use.
4. An EHR will be easier to use if it has single sign-on capability.

Multiple-Access System

1. It will be easier to use an EHR if I can access the system from different computers.
2. It will be easier to use an EHR if multiple users can access the system from the same computer.

3. Being able to access the EHR from different computers will make it easier to use it.
4. Allowing many individual care givers to access the EHR from the same computer will make it easier to use it.

Attitude

1. Using an EHR increases patient satisfaction.
2. Enables to increase customer retention rate.
3. Using an EHR improves the quality of work I do.
4. Using an EHR can effectively segment customer based profitability
5. Using an EHR helps us build relationships with patients.
6. Using an EHR provides differential services to different patients.
7. Using an EMR is based on the consideration for the patient's well being.
8. Using an EMR affects the patient's view of the quality of the facility's operations.
9. Using an EMR can effectively enhance patient satisfaction.
10. Using an EHR improve patient satisfaction.

Behavioral Intention

1. I intend to use an EHR in my job as often as needed.
2. I intend to use an EHR in my job routinely
3. Whenever possible, I intend to use an EHR on my job.
4. To the extent possible, I would use an EHR to do different things.

System Use

1. I use the EHR often.
2. I use the EHR in my job routinely.
3. I use the EHR almost all the time
4. I will use the EMR many hours each day.
5. I use an EMR in my job as often as needed.

Organization Information

1. Number of Beds: _____
2. Occupancy Rate: _____
3. Number of Employees

Respondent Demographics

4. Position
5. Education Level
6. Age
7. Ethnicity
8. Sex
9. Years of experience
10. Computer expertise

Appendix B: Factor Loadings from Preliminary Pilot Study Results

	Att	BehInt	Biomdev	Compatible	Compliance	Ease Of Use	Env	Obs	Trial	Use	Useful	cost	ind	maas	org	sec	sso	task
Att1	0.8695	0.5098	0.233	0.5724	0.313	0.5924	0.6783	0.3255	0.49	0.4075	0.6387	-0.5765	0.3831	0.2225	0.4226	-0.4609	0.1568	0.634
att1	0.9377	0.3999	0.2004	0.6626	0.2242	0.614	0.8057	0.3796	0.6082	0.224	0.7422	-0.6946	0.3212	0.2892	0.434	-0.5902	0.2724	0.7709
att10	0.9216	0.3461	0.1367	0.6137	0.2378	0.5106	0.8545	0.2768	0.5664	0.0805	0.6873	-0.5587	0.3066	0.2449	0.3683	-0.5925	0.2557	0.8036
att3	0.8131	0.5972	0.3204	0.8308	0.169	0.7468	0.7192	0.4202	0.5559	0.3941	0.8828	-0.6333	0.1472	0.4557	0.5006	-0.5073	0.3069	0.6343
att5	0.8247	0.4457	0.2221	0.5936	0.175	0.4782	0.64	0.3187	0.4093	0.4067	0.6249	-0.6038	0.4279	0.1375	0.3861	-0.4596	0.2092	0.609
att6	0.7018	0.505	0.2339	0.4598	0.3115	0.5032	0.5713	0.3353	0.4941	0.1892	0.5445	-0.6294	0.4143	0.387	0.5548	-0.305	0.2859	0.6506
att7	0.786	0.4356	0.2437	0.5598	0.0516	0.5473	0.6601	0.4223	0.4653	0.2964	0.5468	-0.5984	0.2741	0.4602	0.3378	-0.6209	0.2593	0.7221
att8	0.6121	0.3683	0.3528	0.5008	0.2989	0.3741	0.5923	0.1117	0.2712	0.198	0.5561	-0.4017	0.4966	0.2264	0.4617	-0.317	0.308	0.5859
att9	0.8714	0.3266	0.0833	0.5718	0.2466	0.5573	0.7829	0.2451	0.5373	0.0514	0.6339	-0.5896	0.2692	0.2806	0.4444	-0.4984	0.2099	0.7312
bi3	0.3814	0.8088	0.1466	0.5989	-0.0897	0.6535	0.3497	0.6015	0.3117	0.5985	0.5382	-0.3643	0.1696	0.5637	0.5154	-0.5178	0.3864	0.4434
bi4	0.4986	0.8407	0.3371	0.5607	0.0427	0.5855	0.3933	0.5163	0.4937	0.6775	0.5482	-0.4669	0.2579	0.2899	0.4956	-0.3713	0.3772	0.479
biomd1	0.3024	0.2803	0.9048	0.2851	0.4221	0.3203	0.2754	0.2028	0.392	0.1937	0.344	-0.3474	0.4767	0.2625	0.299	-0.1552	0.3386	0.3385
biomd2	0.149	0.1806	0.8726	0.1534	0.4386	0.198	0.0908	0.0695	0.2728	0.0947	0.2414	-0.2677	0.2679	0.2331	0.1912	-0.0584	0.3513	0.1865
biomd3	0.1489	0.2173	0.7063	0.1274	0.2795	0.1943	0.0884	0.126	0.3014	0.1221	0.1172	-0.1832	0.2224	0.2774	0.1951	-0.217	0.3348	0.2101
biomd4	0.2586	0.2883	0.8736	0.2303	0.1977	0.3853	0.2279	0.2211	0.3439	0.3068	0.2689	-0.3238	0.4101	0.2925	0.1921	-0.1867	0.1834	0.2638
comp1	0.4957	0.4886	0.247	0.8115	0.0068	0.5634	0.3805	0.4108	0.2328	0.4669	0.6978	-0.3868	0.1547	0.4618	0.2734	-0.4335	0.41	0.468
comp2	0.6799	0.6287	0.2077	0.9166	-0.0049	0.7606	0.6941	0.4794	0.4601	0.4081	0.8409	-0.5555	0.0685	0.5585	0.5247	-0.5858	0.3644	0.6752
comp3	0.6645	0.6837	0.3345	0.8991	0.1077	0.7959	0.6239	0.4842	0.4815	0.4743	0.8136	-0.4947	0.1733	0.5179	0.486	-0.5471	0.3966	0.5989
comp4	0.704	0.631	0.0895	0.8589	0.0648	0.6402	0.5944	0.3009	0.2692	0.5143	0.7204	-0.5175	0.2991	0.3939	0.4798	-0.3775	0.2215	0.5735
compl2	0.2479	-0.0259	0.2808	0.0603	0.8568	0.1159	0.2737	-0.0283	0.3063	-0.1716	0.1898	-0.0484	0.3101	-0.0539	-0.1019	0.056	0.198	0.1481
compli3	0.1339	0.0437	0.3027	0.0226	0.6837	-0.0872	0.1187	-0.2232	-0.0688	0.0281	-0.0004	-0.2025	0.3699	0.0856	0.1919	0.1351	0.1972	0.021
Compl4	0.1678	-0.0557	0.228	0.0132	0.538	0.1457	0.0351	0.0315	0.1786	-0.0656	0.1759	-0.1442	0.0022	0.0206	-0.0032	0.1584	0.1623	-0.0113
cost1	0.131	0.2838	0.0544	0.1713	-0.183	0.1386	-0.0338	0.2135	-0.0438	0.4137	0.1522	-0.363	0.0194	0.1449	0.2446	-0.2067	0.1885	0.0426
cost3	-0.7277	-0.4531	-0.3291	-0.5554	-0.2121	-0.558	-0.6942	-0.4945	-0.4499	-0.3072	-0.6416	0.9438	-0.467	-0.522	-0.5826	0.4871	-0.352	-0.6459
cost4	0.1563	0.2175	0.1793	0.1307	-0.0205	0.113	-0.0041	0.0981	0.0527	0.2925	0.1014	-0.3699	0.2196	0.1559	0.2002	-0.1203	0.1598	0.0837
env1	0.1855	0.3147	0.2181	0.1762	0.0698	0.2028	0.333	0.0575	-0.0551	0.3483	0.0999	-0.3373	0.3884	0.2522	0.3324	-0.0962	0.0688	0.2001
env2	0.3478	0.41	0.4146	0.4207	0.1499	0.4034	0.5385	0.2675	0.2584	0.2523	0.4222	-0.2893	0.2059	0.5802	0.4117	-0.3903	0.3879	0.4464
env3	0.8458	0.3033	0.052	0.5877	0.1956	0.5474	0.9043	0.2462	0.5096	0.0393	0.6743	-0.5638	0.2478	0.2133	0.438	-0.5424	0.1076	0.7248
eou1	0.6262	0.6494	0.2965	0.6553	0.1294	0.8703	0.5489	0.521	0.4538	0.5766	0.7134	-0.5036	0.2193	0.2715	0.4955	-0.358	0.245	0.4649
eou2rev	0.1188	0.2289	-0.0632	0.19	0.0389	0.2597	0.1125	0.1959	0.1408	0.0581	0.2789	-0.0747	-0.3143	0.0545	0.1593	-0.1154	0.0723	0.1161
eou3	0.4654	0.6742	0.2742	0.6493	-0.0158	0.8983	0.4724	0.6769	0.5032	0.5887	0.5981	-0.4424	0.0938	0.4549	0.4816	-0.4529	0.2798	0.4235
eou5	0.609	0.5594	0.3036	0.4819	0.2024	0.6909	0.5334	0.4302	0.6236	0.3715	0.5223	-0.3177	0.1239	0.2751	0.2501	-0.4256	0.271	0.5908
eou7	0.6998	0.6536	0.3227	0.8276	0.1437	0.8975	0.6382	0.5598	0.3927	0.5457	0.7692	-0.6195	0.3126	0.5471	0.5775	-0.4824	0.3316	0.5837
eou4	0.5608	0.6505	0.3618	0.7214	0.0524	0.9114	0.5402	0.551	0.3978	0.5368	0.6741	-0.5468	0.1331	0.5888	0.5517	-0.4047	0.28	0.4916
eou6	0.5414	0.6912	0.2953	0.7565	0.0303	0.9076	0.5449	0.5542	0.3968	0.5701	0.6737	-0.4364	0.2083	0.5071	0.549	-0.4513	0.2179	0.4966
ind1	0.1383	0.2474	0.2237	0.0624	0.1165	0.0603	0.1169	0.0107	0.0932	0.3378	0.0685	-0.2793	0.6559	0.1279	0.3316	-0.1723	0.202	0.1189
ind3	0.3217	0.1733	0.3062	0.1565	0.2335	0.1886	0.3667	0.2586	0.1615	0.1305	0.1621	-0.3369	0.7272	0.2827	0.1857	-0.2834	0.3211	0.3184
ind4	0.3459	0.1937	0.3811	0.1722	0.2952	0.1455	0.2177	0.0337	0.2671	0.2814	0.3033	-0.4016	0.7993	0.0707	0.2061	-0.0006	0.2343	0.2972
mas1	0.1457	0.3135	0.2909	0.2972	-0.0301	0.2528	0.1835	0.186	-0.0554	0.1583	0.1861	-0.3246	0.1629	0.7927	0.387	-0.2055	0.3556	0.2798

mas2	0.2219	0.2726	0.2864	0.2623	0.3275	0.2314	0.2089	0.2015	0.1815	0.1084	0.2632	-0.3638	0.2481	0.6174	0.2499	-0.1439	0.4493	0.2493
mas3	0.3713	0.5249	0.1879	0.6044	-0.1681	0.5761	0.4429	0.4164	0.1854	0.3432	0.4835	-0.4698	0.1007	0.8909	0.5579	-0.4662	0.4275	0.5241
mas4	0.2646	0.1275	0.3207	0.1372	0.2752	0.1172	0.2673	0.1984	0.1472	0.1356	0.234	-0.3792	0.366	0.3795	0.1575	-0.2353	0.3878	0.3172
obs2	0.1456	0.3397	0.232	0.2153	0.0282	0.3373	0.1208	0.6851	0.4061	0.3448	0.2343	-0.2075	0.0634	0.216	0.0756	-0.4059	0.2793	0.2382
obs3	0.4305	0.6095	0.1048	0.5129	-0.1306	0.5971	0.3319	0.9173	0.5518	0.5471	0.4993	-0.5332	0.1305	0.3679	0.2896	-0.5285	0.3963	0.4871
obs4	0.2975	0.6669	0.246	0.3752	-0.0286	0.5846	0.2424	0.8784	0.4332	0.6251	0.4245	-0.4202	0.1873	0.3682	0.4039	-0.5163	0.3468	0.3313
org1	0.5525	0.6046	0.2807	0.5378	0.1002	0.6213	0.5782	0.3403	0.2975	0.2917	0.5345	-0.5942	0.2384	0.5787	0.9387	-0.3582	0.2203	0.4908
org2	0.2818	0.3916	0.1254	0.2693	-0.1971	0.2489	0.3287	0.2051	0.08	0.3636	0.2309	-0.4203	0.2909	0.2828	0.7369	-0.2596	0.0177	0.2155
pu	0.6459	0.7125	0.3136	0.879	0.1149	0.7677	0.5502	0.5055	0.3849	0.6563	0.8708	-0.5762	0.2669	0.5091	0.5179	-0.4894	0.4392	0.5508
pu1	0.6905	0.534	0.2212	0.7263	0.1152	0.6195	0.6107	0.4095	0.5261	0.292	0.8917	-0.5265	0.2497	0.3606	0.4837	-0.402	0.3619	0.6382
pu3	0.6968	0.6196	0.3491	0.7938	0.1573	0.7366	0.6298	0.5357	0.6031	0.4655	0.8669	-0.5959	0.1929	0.3965	0.3792	-0.5353	0.4015	0.5999
pu4	0.7885	0.5118	0.2459	0.7771	0.2261	0.621	0.6976	0.3737	0.4741	0.3657	0.9401	-0.6221	0.3078	0.3824	0.3973	-0.4817	0.4021	0.6554
pu8	0.717	0.634	0.2829	0.8094	0.187	0.7245	0.6756	0.4919	0.5634	0.433	0.9581	-0.5704	0.2587	0.4534	0.4909	-0.486	0.4359	0.6275
pu9	0.8261	0.5622	0.2362	0.8139	0.2523	0.7222	0.7849	0.383	0.5567	0.2726	0.9192	-0.5631	0.2337	0.3911	0.432	-0.4999	0.3062	0.7292
sec1	-0.0213	-0.1541	0.0636	-0.0666	0.2223	-0.175	-0.1039	-0.1947	0.028	-0.1855	-0.0924	0.0118	0.0196	-0.1105	0.0403	0.1475	-0.1259	-0.0653
sec2rev	-0.6023	-0.5308	-0.1854	-0.5665	0.1362	-0.4876	-0.6052	-0.5721	-0.5508	-0.4009	-0.5338	0.5096	-0.2025	-0.4254	-0.3715	0.9981	-0.4626	-0.7306
sec3	0.0148	-0.0601	0.0814	-0.039	0.0891	-0.0017	0.0171	0.0454	-0.0077	-0.075	-0.0457	-0.0898	0.0398	0.1129	0.2305	0.0701	-0.1365	-0.0465
sec4	-0.0293	-0.1876	-0.1075	-0.0452	0.1869	-0.2015	-0.0988	-0.2478	-0.178	-0.1385	-0.1173	0.0342	0.1622	0.0343	-0.0764	0.3121	-0.0522	-0.1162
sso1	0.3458	0.4207	0.2969	0.3972	0.1737	0.2979	0.2671	0.4124	0.3095	0.4052	0.4904	-0.4262	0.4324	0.4078	0.1823	-0.4322	0.868	0.4552
sso3	0.158	0.3427	0.2372	0.243	0.2677	0.2241	0.1318	0.2713	0.2982	0.1608	0.1971	-0.202	0.1249	0.4916	0.1113	-0.321	0.7677	0.3851
sso4	-0.0872	0.1418	0.2995	0.1387	0.167	0.0249	-0.1763	0.0552	-0.0485	0.0913	0.0621	0.0185	0.012	0.3264	-0.0663	-0.1332	0.5722	0.065
su1	0.3318	0.7236	0.2342	0.5556	-0.0703	0.6463	0.2284	0.6736	0.2309	0.9155	0.5162	-0.4597	0.2926	0.299	0.3696	-0.422	0.3466	0.2551
su2	0.2581	0.7181	0.225	0.4349	-0.0917	0.544	0.1344	0.5736	0.2303	0.9615	0.4053	-0.3488	0.3304	0.2322	0.3116	-0.3059	0.3077	0.2058
su3	0.2497	0.7125	0.2208	0.4453	-0.0648	0.5356	0.1346	0.5064	0.2388	0.9418	0.4237	-0.3024	0.3265	0.1925	0.2817	-0.348	0.3347	0.2097
su4	0.2599	0.7314	0.2358	0.5393	-0.1723	0.5569	0.1491	0.5452	0.271	0.8653	0.3778	-0.3316	0.1952	0.3709	0.3532	-0.3614	0.329	0.235
su5	0.3093	0.6697	0.173	0.4609	-0.1843	0.5206	0.1955	0.5656	0.2244	0.9089	0.3843	-0.4362	0.2779	0.3266	0.351	-0.4284	0.3228	0.2679
task1	0.8799	0.5067	0.3252	0.6523	0.2265	0.5824	0.8557	0.3324	0.5278	0.182	0.7113	-0.6687	0.3767	0.5279	0.5409	-0.6119	0.4505	0.9442
task2	0.5727	0.5144	0.2254	0.5261	-0.1273	0.454	0.5262	0.5301	0.6125	0.3158	0.5039	-0.3908	0.2972	0.3747	0.2212	-0.7368	0.4553	0.8544
task3	0.0637	0.029	-0.1181	0.1846	0.0038	0.0819	-0.0085	0.0893	-0.1458	-0.0405	0.1715	-0.0961	-0.1965	0.1443	0.0548	-0.0238	0.1449	0.0984
trial1	0.4876	0.4304	0.3873	0.3514	0.2764	0.3882	0.3334	0.4051	0.8525	0.2357	0.4789	-0.2781	0.2563	0.118	0.1719	-0.4582	0.3826	0.4474
trial2	0.4318	0.3848	0.3853	0.2924	0.2607	0.3907	0.388	0.4467	0.8695	0.1666	0.4448	-0.3751	0.3059	0.1261	0.2432	-0.457	0.318	0.4659
trial3	0.6008	0.4398	0.2655	0.4175	0.1192	0.5369	0.5406	0.5685	0.8475	0.253	0.525	-0.406	0.1381	0.1789	0.2427	-0.488	0.2287	0.6171