Communications of the Association for Information Systems

Volume 31 Article 9

12-2012

Ubiquitous Healthcare Information System: Toward Crossing the Security Chasm

Humayun Zafar
Kennesaw State University, hzafar@kennesaw.edu

Sweta Sneha
Department of Information Systems, Kennesaw State University

Recommended Citation
Zafar, Humayun and Sneha, Sweta (2012) "Ubiquitous Healthcare Information System: Toward Crossing the Security Chasm," *Communications of the Association for Information Systems*: Vol. 31 , Article 9.
DOI: 10.17705/1CAIS.03109
Available at: https://aisel.aisnet.org/cais/vol31/iss1/9

Communications of the Association for Information Systems

CAIS

Ubiquitous Healthcare Information System: Toward Crossing the Security Chasm

Humayun Zafar

Department of Information Systems, Kennesaw State University

hzafar@kennesaw.edu

Sweta Sneha

Department of Information Systems, Kennesaw State University

Abstract:

Ubiquitous healthcare information system is increasingly seen as a viable option for reducing the inherent time lag and inaccuracies in the traditional model of healthcare and promoting the delivery and practice of evidence-based healthcare—as and when needed—without any location and time constraints. Although promising, the realization of ubiquitous healthcare information system brings several threats and risks rooted in real-time collection, analysis, storage, transmission, and access of critical medical data. In this research, we address information security concerns pertaining to the paradigm of ubiquitous healthcare information system. To accomplish this we use National Institute for Standards and Technology's (NIST's) system development lifecycle model (SDLC) as the underlying framework to explore the current state of ubiquitous healthcare from the perspective of security. We then leverage the model to propose future research directions in this area. By implementing the NIST's SDLC model in such a manner, we offer a different dynamic of healthcare security that has not been addressed in literature before.

Keywords: enterprise wide systems, pervasive systems, and security

Editor's Note: The article was handled by the Department Editor for Information Systems and Healthcare.

Volume 31, Article 9, pp. 193-206, December 2012

Communications of the Association for Information Systems

I. INTRODUCTION

The concept of "Ubiquitous Healthcare" originated from Mark Weiser's vision, which was captured as: "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" [Weiser, 1991]. The vision of Mark Weiser translated to the healthcare domain holds the promise of an environment that flawlessly integrates ubiquitous computing, communication, and sensing technologies in everyday objects, thereby facilitating the delivery of healthcare services that focus on wellness, disease management, and support for independent living for everyone, everywhere, without any dependence on time and location [Kidd, Orr, Abowd, Atkeson, et al., 1999; Mynatt, Essa, and Rogers, 2000; Sneha and Varshney, 2009; Stanford, 2002]. The notion of ubiquitous healthcare entails a paradigm shift in healthcare practice, delivery and view focusing on patient-centric operational models promoting real time monitoring of patients' medical progress, compliance to physicians' advice such as taking prescription drugs as and when required, and prompt detection of anomalies without time and location dependencies [Floerkemeier and Siegemund, 2003; Korhonen, Paavilainen, and Särelä, 2003a].

The recent advancement in three classes of technology—communication, computing, and sensing—have laid the foundation for the development of information systems enabling ubiquitous healthcare and the emergence of ubiquitous healthcare as a research discipline [Kitsios, Papadopooulos, and Angelopoulos, 2010]. The fundamental process of ubiquitous healthcare involves sensing of patient specific information such as vital signs, drug compliance, etc., analysis of collected information for detection of anomalies, and communication of pertinent information to healthcare stakeholders (doctors/nurses/relevant family members) as and when required (Figure 1). The scope of a dedicated ubiquitous healthcare information system (UHIS) encompasses (a) pervasive monitoring of patients based on data collected from multiple sensors/computing devices, (b) authorized real-time access of context specific healthcare information, (c) prompt detection of anomalies, (d) provision of real time medical feedback and pertinent decision support to authorized stakeholders (such as doctors, nurses, family members) irrespective of the geographical and time constraints. Consider the case of an aging cardiac patient living in his/her home (Figure 1). UHIS can enable continuous monitoring of patient specific vital signs such as ECG, send reminders to ensure medication compliance, send real time feedback to the patient on his/her daily progress, send alerts to doctors, nurses, etc. if an anomaly is detected in the reading of the vital signs so that appropriate medical intervention can be provided. UHIS also enables authorized users access to relevant medical data of the patient. The data can be utilized for trend analysis, detection of critical changes in vital signs, and provision of evidence-based healthcare rooted in factual data collected from biometric sensors and other computing devices.

The paradigm of ubiquitous healthcare seeks to shift the focus from treating sickness to promoting proactive wellness and independent living. Technologies promoting wellness range from blood pressure cuffs and glucose meters that can upload information to a personal computer, to professional caregivers [Borriello, Stanford, Narayanaswami, and Menning, 2007]. Information systems empowered by ubiquitous computing, communication, and sensing technologies also support healthy independent living of older adults outside the hospital in their own environment via wearable sensors, infrared badges, wheelchairs, package blister packs, java smartphones, and multi-modal sensors in futuristic smart homes, etc. [Floerkemeier and Siegemund, 2003; Helal, Giraldo, Kaddoura, Lee, et al., 2003; Korhonen et al., 2003a; Sneha and Varshney, 2009]. Environments leveraging ubiquitous technologies assist visually impaired users in leading an independent life by conversing with them [Coroama and Röthenbacher, 2003]. Bardram [2003] describe a scenario in which ubiquitous computing technology will become an integral element of prescription drugs, thereby providing information related to the effectiveness and adverse interaction of medications, promoting compliance via alerts/reminders, keeping relatives and doctors/nurses abreast of elderly patients' drug compliance and progress [Floerkemeier and Siegemund, 2003]. Ubiquitous access of context specific medical information by doctors and nurses is increasingly seen as a viable option for reduction in the inherent lags and inaccuracies in the traditional healthcare workflow, early detection of anomalies, reduction in preventable hospitalizations and corresponding expenses, and prompt provisioning of pertinent medical intervention "just in time" as and when needed [Joo–Hak, 2008; Korhonen, Parkka, and Van Gils, 2003b; Omary Mtenzi, Wu, and O'Driscoll, 2011].

The realization of the enhanced effectiveness and efficiency in healthcare delivery and practice associated with UHIS requires collection, processing, transmission, and storage/access of sensitive patient information, which in turn leads to critical security threats and risks. The enhanced functionalities afforded by ubiquitous computing,

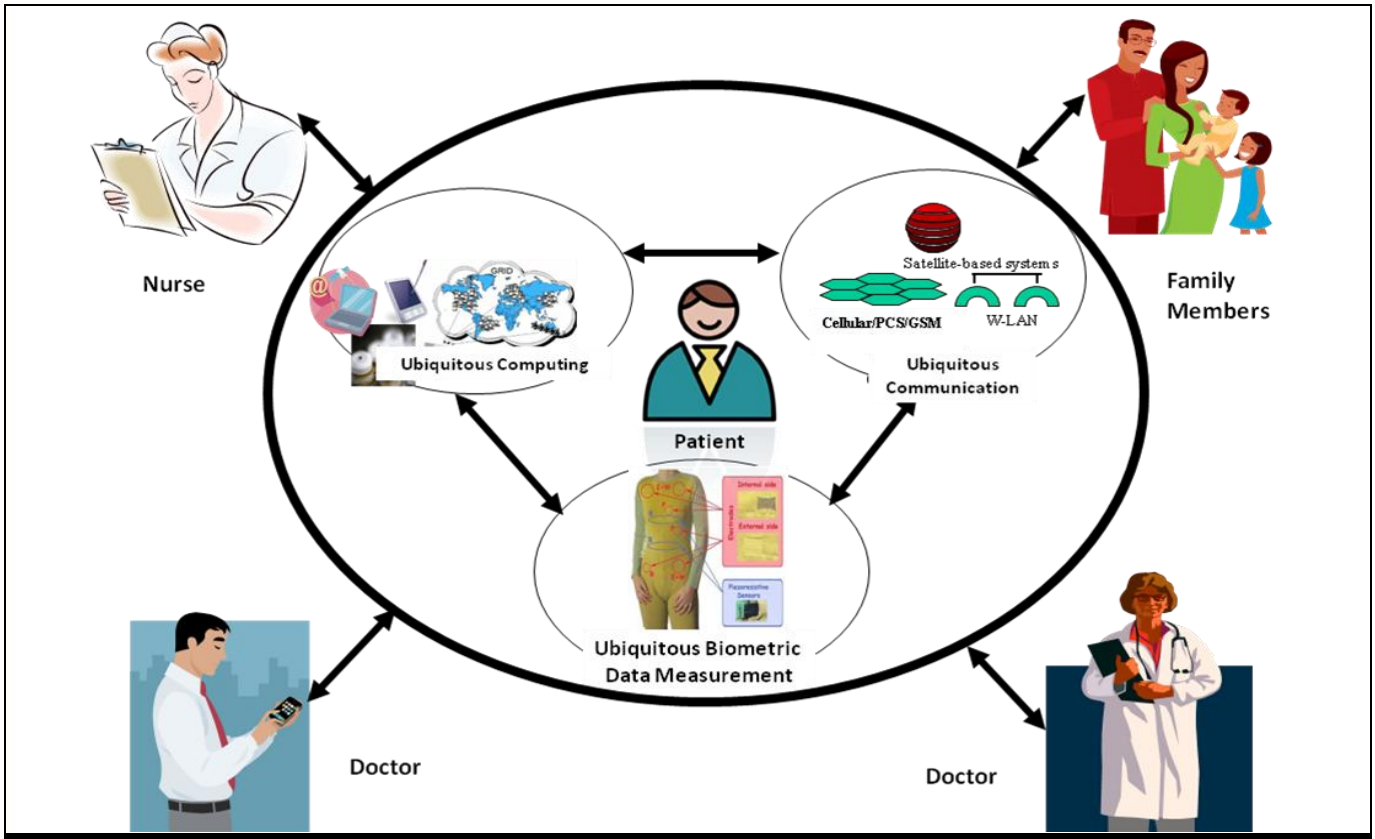

Figure 1. Conceptual Model of Ubiquitous Healthcare Environment

communication, and sensing technologies bring increased challenges with respect to data storage, distribution, connectivity, computational power, and energy budgets [Liu, Clark, and Stepney, 2005]. Additionally, the ubiquity of information access further accentuates security concerns associated with potential abuse [Bohn, Gärtner, and Vogt, 2004]. Dealing ethically with critical patient information derived from biometric sensors and mobile devices require systems to not only be reliable and scalable but also to maintain the confidentiality, integrity, and privacy of sensitive health data. Cisco in its annual report for 2010 predicted that attackers will increasingly target mobile devices as they make their way onto enterprise networks [Cisco, 2011]. This prediction was not too dissimilar from earlier ones [Leavitt, 2005]. The reason the landscape did not change appreciably before was because mobile devices were not attractive and/or lucrative targets for attackers, due to the heterogeneous nature of the technologies involved. Malware development for a single platform did not result in a high number of victims, and altering malware for use on multiple platforms was not as cost effective. However, as mobile devices become homogenous in terms of operating system usage and the backbone networking technologies [Ahmed, Jamal, Mehboob, Khan, et al., 2010], with popular and full-featured SDK APIs, creation of malware will become comparatively trivial, thereby leading to information security concerns. Besides, it is to be noted that wireless communication channels suffer from spotty coverage and are not 100 percent reliable [Sneha and Varshney, 2009]. The sole reliance of ubiquitous healthcare information systems (UHIS) on wireless channels for data communication/transfer provides further opportunities to malicious agents [Liu et al., 2005].

Hence, it is critical that the increased vulnerabilities associated with UHIS (in terms of ubiquitous access, enhanced mobility, wireless communication, power constraints, etc.) are appropriately assessed and managed. Unfortunately, there is a dearth of methodical guidelines for tackling the burning security concerns in the context of UHIS. Von–Solms [2006] defines information security as a phenomenon that occurs in waves, progressing from technical to managerial to institutional and finally to information security governance. Problems related to information security can be behavioral, managerial, philosophical, and/or organizational. Therefore, we need to consider a more holistic view of information security, incorporating technology, processes, and people [Baskerville, 1993; Da Veiga and Eloff, 2007; Dhillon and Torkzadeh, 2006; Straub and Welke, 1998]. Healthcare IT is no different. Considering the inherently private and sensitive nature of the data involved, a holistic approach is needed toward UHIS [Rajan and Ramaswamy, 2010]. It is critical that system designers incorporate security in the design of UHIS at multiple different phases in order to ensure that the characteristic risks associated with UHIS can be mitigated. In the current research, we specifically investigate security concerns associated with UHIS with the objective to (a) have a holistic

Communications of the Association for Information Systems

understanding of the landscape of UHIS research in the context of security and (b) provide a frame of reference to UHIS designers/developers toward incorporating security in UHIS.

We leverage the National Institute for Standards and Technology's (NIST's) system development lifecycle model (SDLC) as the underlying framework to explore the current state of UHIS from the perspective of security and to assess future research directions. The analysis reveals that, so far, the majority of the work has focused on the technical aspects of security. The next section presents a brief overview of NIST, the security guidelines incorporated in each phase of the SDLC model, and the current state of UHIS research with respect to security. Section III discusses the gaps in the current landscape of security research in UHIS and presents the direction of future research. Section IV concludes the article.

II. THE NIST INFORMATION SECURITY AND THE SYSTEM DEVELOPMENT LIFECYCLE MODEL (SDLC)

NIST develops standards and guidelines for providing adequate information security for an agency's operations and assets. The security considerations in the system development lifecycle have been developed to assist in integrating an organization's essential IT security steps into their established IT infrastructure [Kissel, Stine, Scholl, Rossman, et al., 2008]. Unlike some of the comparable security models, such as the ISO 27000 series, NIST documents are publicly available, free, and have been available for a while. They have also been broadly reviewed by government and industry professionals and were among the first references cited by the federal government when it decided not to select the ISO/IEC 17799 standards [Holden, 2003].

Kissel et al. [2008] state that information security processes and activities provide insights into managing systems and their development. They also enable risk identification, planning, and mitigation. A risk management approach needs to continually balance protection of assets with costs associated with the task. The importance of undertaking a risk management approach in healthcare has been highlighted by Landry, Pardue, Johnsten, Campbell, et al. [2011], who created a threat tree for healthcare information privacy and security. Kissel et al. [2008] further mention that in order to have effective risk management for systems, security needs to be integrated early and throughout an organization's established systems and lifecycles. This integration enables security to be planned, acquired, and deployed as an essential component of a system. Clark, Beebe, Williams, and Shepherd. [2009] support this notion by stating that systems can attain reasonable levels of security if the design team addresses these issues in the early stages of design, progressing through the life of the system. After all, most security attacks to systems can be attributed to poor systems design [Hoglund and McGraw, 2004; McGraw, 2004].

Kissel et al. [2008] incorporate security into the linear sequential model of SDLC, and consider it as an appropriate platform for a NIST model. However, the authors also mention that the concepts in this model can be adapted to any SDLC model. A linear sequential model contains five phases: initiation, development, implementation, maintenance, and disposal [Khalifa and Verner, 2002]. In each phase, Kissel et al. [2008] present a minimum set of security tasks needed to effectively incorporate security in the system-development process. The proceeding sections explore how the current state of UHIS research addresses the key security activities incorporated in each of the SDLC phases.

Initiation

In this phase requirements about a system are gathered. This is a critical phase because misinterpretation at this stage may give rise to problems later. Therefore, it is important to understand the requirements and expectations so that the end result meets all specifications. The NIST guidelines mirror this point by stating that security considerations are key to diligent and early integration [Kissel et al., 2008]. Key security activities for this phase are threefold:

- Delineation of business requirements in terms of confidentiality, integrity, and availability
- Categorization and identification of information of known special handling requirements (e.g., personally identifiable information) to transmit, store, or create information
- Determination of privacy requirements

Business outcomes can be assessed in multiple ways. First, identification of core system components needed to maintain minimal functionality. Second, identification of the maximum period that the system can be down before the business itself is impacted. Finally, lines of business supported by the system and how those lines are impacted need to be identified.

Information categorization provides a strong linkage between a system and cost-effective information security. In this phase information can be categorized through specification of high level security requirements, a detailed system security plan that documents key decisions, and supporting rationale for the IT security procedures.

Privacy requirements can be assessed through details about where and to what extent private information is collected, stored, or created within the system. This includes processes developed to address privacy information incident handling and reporting requirements according to any laws and regulations that may exist.

Previous research in healthcare IT security has focused quite a bit on keeping information private as regulated by legislations such as Health Insurance Portability and Accountability Act [HIPAA, 1996], the Privacy Act of 1974 [FPA, 2007], the HITECH Act [Blumenthal, 2010], and ARRA [Grumbach and Mold, 2009]. Rindfleisch [1997] found that continued development of enterprise-wide IT systems in healthcare was a doubled-edged sword. On one hand it was an essential development since it provided for optimal healthcare. However, it would also inevitably lead to threats, such as intentional and unintentional healthcare information disclosure from insiders, as well as from external intruders. Some have argued that legislations such as HIPAA have in fact created more security risks [Mercuri, 2004].

UHIS has also been considered to be a means of increasing healthcare productivity of practitioners, while also facilitating delivery of a wider range of medical services. Yet security and privacy concerns associated with transmission and storage of data have been highlighted [Varshney, 2003]. Stanford [2002] highlighted the fact that growth in ubiquitous healthcare technology has to correlate with the legal environment in which these tools operate. According to the author, this is especially true regarding adapting ubiquitous technologies to legislative acts such as HIPAA. Halperin [2008] stated that although security and privacy were legitimate concerns in regard to ubiquitous healthcare technologies, balance between security and usability needed to be achieved.

Development

In this phase requirements are broken down into logical module for ease of implementation. Kissel et al. [2008] recommend the following to be key security activities of this phase:

- Conducting a risk assessment and developing a security baseline
- Designing a security architecture

A risk assessment is based on an already established system that reflects its potentials risks and known weaknesses. Although research has been carried out in regard to the importance of risk assessments in enhancing healthcare IT in general [Eloff and Eloff, 2005; Jepsen, 2003; Matuleviius, Mayer, Mouratidis, Dubois, et al., 2008], risk assessments have not been explored in relation to ubiquitous healthcare IT security. Security risk assessments of ubiquitous healthcare devices is just as important in relation to establishing a secure healthcare infrastructure [Janczewski and Xinli Shi, 2002]. A point to note is that provision of infrastructure services is an enabling mechanism. Though the infrastructure itself will yield benefits, the core requirements will be achieved by the provision of additional applications and services. That in itself makes execution at the initiation level critical.

Designing a secure architecture for UHIS is an important task since it requires a high degree of interoperability among shared devices and services. A clear plan is needed to plan these services and understand how they will be integrated into the system. At the managerial level the designed architecture should ensure that the initiative fits an organization's vision and does not conflict with existing services or provide redundant ones. At the system level security can be established through clustering services or distributed for either redundancy or additional layers of protection [Kissel et al., 2008]. Both in regard to healthcare IT security and ubiquitous device security, there has been a reasonable discussion on the technical aspects of a security architecture [Eloff and Eloff, 2005; Gritzalis and Lambrinoudakis, 2004; Murphy and Chueh, 2002; Ng, Sim, and Tan, 2006]. The relationship between interoperability and security still needs to be addressed [Brailer, 2005].

Implementation

In this phase the system is installed and evaluated in an organization's operational environment. They key security activity includes:

- Integration and assessment of the system in its environment

System integration occurs at the deployment site for the system. At this stage the expected output is a verified list of operational security controls. The implemented system has to be assessed in order to validate that it complies with the functional and security requirements and that it will operate within an acceptable level of residual security [Kissel

et al., 2008]. Prior research on implementation in both the healthcare IT and ubiquitous device security has concentrated on the technical aspects of implementation of technologies [Dwivedi, Bali, Belsis, Naguib, et al., 2003; Epstein, Pasieka, Lord, Wong, et al., 1998; Hu and Weaver, 2004; Kardas and Tunali, 2006; Ng et al., 2006].

Researchers have recognized that with ubiquitous Internet accessibility remote patient monitoring has become a viable option for people responsible for providing in-home healthcare management. For example, Kara [2002] states that the Internet's transport and network layers are a primary concern and presents a case for the use of Internet protocol security (IPSec) to provide network-layer security without limiting the Internet's ubiquity. The usefulness of IPsec with regard to security ubiquitous device security has also been discussed by Korhonen et al. [2003b]. The authors state that the adoption of IPv6 in the future will lead to data integrity and protection and enhanced security, since IPv6 connections always used the IPSec protocol.

Venkatasubramanian and Gupta [2006] focus on maintaining the security of wearable networked health monitoring sensors, also known as Body Sensor Networks (BSN), and present means of using physiological values from the wearer's body for securing inter-sensor communication. Warren, Lebak, Yao, Creekmore, et al. [2005] echoed this study and focused on the development of health and activity monitors that utilized ZigBee wireless connectivity and hardware-level encryption in a BSN.

Maintenance

In this phase, the assumption is that the system has already been developed and deployed. Key security activities in this phase include:

- Continuous monitoring of the system's security controls for operational readiness
- Managing the configuration of the system

In an operational environment that is as fluid as IT, changes are bound to occur. This may require a change in the security controls, such as configurations, to ensure the system's integrity. Changes need to be documented and assessed. The monitoring itself can be done in a variety of ways. Security reviews, self-assessments, and patch management are just some of the examples [Kissel et al., 2008].

Both healthcare IT and ubiquitous device security are relatively new research areas. Therefore, most of the concerns with regard to maintenance of technologies to achieve enhanced security have been expressed in terms of updating healthcare security standards of applications [Kokolakis and Lambrinoudakis, 2005], employing new hardware and software techniques [Giakoumaki, Perakis, Tagaris, and Koutsouris, 2008], and developing new platforms for healthcare IT in general [Shoniregun, Dube, and Mtenzi, 2010; Su and Al-Hakim, 2010].

Despite advances in technology and considerable research in the technical aspects of such technologies, our understanding of how ubiquitous device security and privacy interact with and affect medical safety and treatment effectiveness is still limited [Halperin et al., 2008].

Disposal

The final phase provides for the secure disposal of the system. Information security issues associated with this phase need to be stated explicitly. In most cases, there is no definitive end to a system, as it usually evolves with time. Therefore, system security plans should evolve as well. Key security activities for this phase include:

1. Building a transition/disposal plan
2. Archival of critical data
3. Sanitization of media, and disposal of hardware and software

Building a transition/disposal plan through extensive security documentation ensures that all stakeholders are aware of the future plan for the system and information. Part of the future plans should include a plan for preservation (archiving) of critical data. This could be achieved through indexing of preserved information, its location, and its retention attributes. This may be critical, since methods required for retrieving information in the future may not be readily available [Kissel et al., 2008].

Media sanitization deals with disposal, clearing, purging, and destruction of hardware and software that contains critical data [McCallister, Glance, and Scarfone, 2010]. The sanitization procedures may be more complex, depending on factors such as risk to confidentiality and future plans for the media. Once sanitized, it is possible that

hardware and software may be sold, given away, or discarded, as provided by applicable law or regulation [McCallister et al., 2010].

Researchers have only recently begun to focus on the requirements for disposing of healthcare IT-related products in a secure manner [Farzandipour, Sadoughi, Ahmadi, and Karimi, 2010; Page, 2010; Park, Seo, Son, Lee, et al., 2010; Smith, 2010]. This research has mostly focused on the overall nature of secure disposal of hardware and software, and it not specific to ubiquitous devices. This provides an avenue for future research.

III. FUTURE RESEARCH

The previous sections highlighted the paucity of information security-related research pertaining to UHIS. The lack of information security research in this area is not entirely surprising, since IS as a field has had to deal with the same issue [Zafar and Clark, 2009]. Considering the different phases of the NIST model and their underlying requirements, we identify the following areas for future research.

Initiation

Past research has mostly focused on ensuring that healthcare IT meets the requirements set out by HIPAA regulations. Many researchers have identified the need to focus on the security of UHIS [Kang, Lee, Ko, Kang, et al., 2006]. Legal aspects of UHIS and the need to regulate the UHIS landscape have also been identified [Venkatasubramanian and Gupta, 2007]. However, there is a need to better identify the reasoning behind adoption of UHIS [Ford, Menachemi, and Phillips, 2006; Poon, Jha, Christino, Honour, et al., 2006]. For example, apart from improving the quality of healthcare, can it potentially support public healthcare initiatives? Does it assist with bio-surveillance? Issues pertaining to emerging diseases, bioterrorism threats, and automated reporting need to be addressed [Cole, 2000; Leitenberg, 2005]. Issues pertaining to threats such as terrorism have been covered under Presidential Directive/NSC-63. The directive, which was later updated by the 2003's Homeland Security Presidential Directive 7, mandates that public and private sectors share information about the physical and security threats and vulnerabilities faced by organizations. This led to the creation of various Information Sharing and Analysis Centers (ISACs). Currently ISACs exist for sectors such as financial services and water. As the UHIS landscape evolves, the presence of various vendors and other stakeholders would open itself to threats that will need to be addressed in a manner similar to what ISACs offer.

Development

Past research has explored the importance of risk assessments in enhancing healthcare IT in general. However, risk assessments have not been explored in relation to ubiquitous healthcare IT security. Security risk assessments of ubiquitous healthcare devices is just as important in relation to establishing a secure healthcare infrastructure. Both in regard to healthcare IT security and ubiquitous device security, there has been a reasonable discussion on the technical aspects of a security architecture. The relation between interoperability and security still needs to be addressed [Kang, Kang, Lee, Ko, et al., 2007]. As stated earlier, implementation of the architecture itself is not itself advantageous as opposed to the enabling technologies. Development may include increased transmission through enhanced optical fiber networks, increased capacity, enhanced biomedical databases, and user-centered designs [Casalino, Gillies, Shortell, Schmittdiel, et al., 2003; Chaudhry, Wang, Wu, Maglione, et al., 2006]. Focus on these aspects of UHIS will lead to not just an effective utilization of resources and information, but will also result in the creation of comprehensive risk assessments.

Implementation

Prior research in implementation in both the healthcare IT and ubiquitous device security has concentrated on the technical aspects of implementation of technologies. Researchers have recognized that, with ubiquitous Internet accessibility, remote patient monitoring has become a viable option for people responsible for providing in-home healthcare management. Many researchers have explored the usefulness and the utility of Internet Protocol security in the context of UHIS. Research has also been conducted in the areas of BSN. We contend that healthcare researchers need to further explore healthcare industry and technical standards such as HL7 (HL7 Reference Information Model, and HL7 Clinical Document Architecture) [Kawamoto and Lobach, 2007], Continuity of Care Record (CCR) [Ferranti, Musser, Kawamoto, and Hammond, 2006], and the Unified Medical Language System (UMLS) [Bodenreider, 2004]. Focus on the mentioned standards would allow for integration of UHIS policies with actual compliance. At an organizational level these standards may be informal or formal. Either way, UHIS security will be enhanced.

Managing access control of critical patient information is crucial to successful implementation and adoption of UHIS. There is a need to explore both technical and nontechnical solutions to ensure authorized access to patient information. Role-based and activity-based access control mechanisms have previously been explored to organize

access control and simplify security administration in the healthcare domain [Le, Lee, Lee, Lee, et al., 2010; Zhang and Parashar, 2004]. However, the dynamic nature of the UHIS environment poses multifaceted challenges that requires investigating contextual aware solutions for implementing secure information access control.

Maintenance

Most of the concerns with regard to maintenance of technologies to achieve enhanced security have been expressed in terms of updating healthcare security standards of applications, employing new hardware and software techniques, and developing new platforms for healthcare IT in general. Despite advances in technology and considerable research in the technical aspects of such technologies, our understanding of how ubiquitous device security and privacy interact with and affect medical safety and treatment effectiveness is still limited.

Researchers will also need to explore the scalability of an existing system. Questions pertaining to that area that need to be addressed include suitability for deployment in organizations of varying size, and its ability to interoperate with other healthcare solutions. Systems integration involves the ability to seamlessly share data and resources across all the different systems in an organization. This raises an interesting security issue, because an UHIS may be exposed to a vulnerability if they come in contact with a system that is not completely secure. A system is only as secure as its weakest link [Varian, 2004].

Disposal

Researchers have only recently begun to focus on the requirements for disposing healthcare IT-related products in a secure manner. This research has mostly focused on the overall nature of secure disposal of hardware and software, and it is not specific to ubiquitous devices. This provides an avenue for future research. Of all the phases of the SDLC, this is the most underexplored one. This is not a surprise since UHIS security research is very much in its infancy. Therefore, additional research can be conducted in areas pertaining to the reuse of components and collaborative development. This is an important area of research since federal and state laws require data sanitization, which includes a variety of data eradication methods [Hughes, Coughlin, and Commins, 2009]. Lack of sanitization methods may lead to situations where personal data on the ubiquitous devices is vulnerable to abuse.

IV. CONCLUSION

There are few other domains where life and death depend on obtaining the right information at the right time. Ubiquitous healthcare information systems afford the possibility of an environment that seamlessly integrates computing, sensing, and communication technologies toward pervasive monitoring of patients, anytime/anywhere access of pertinent medical information to authorized stakeholders (e.g., doctors, nurses, family members), real-time feedback and expert advice, prompt detection of anomalies, and provision of medical intervention as and when required without any location and/or time dependencies. There are colossal challenges and opportunities inherent in the realization of UHIS. In this article, we investigated the security aspect of UHIS from the lens of the NIST model.

The ubiquity of mobile computing devices such as iPad, smartphones, advancements in wireless networks, and availability of biometric sensors/nodes have laid the foundation for UHIS. However, it has also created new security threats associated with the collection, storage, transmission, access, and processing of critical medical data. Security issues for systems ultimately concern relationships among social actors—stakeholders, system users, potential attackers, and the software/hardware acting on their behalf [Liu, Yu, and Mylopoulos, 2003]. Many researches in the past have investigated the issue of security of UHIS from the perspective of the mobile computing, communication, and sensing technologies; however, the issue is far from being resolved.

The objective of this article is to leverage the NIST model to assess the landscape of UHIS research from the perspective of security and to lay the direction of future research efforts based on the identification of gaps in the current research. Based on our assessment of UHIS research with respect to security, we find that the majority of prior work focuses on the technical side of security, leaving a wide domain of behavioral and organizational security issues needing more research. Furthermore, the systematic inclusion of security in the design and development of ubiquitous healthcare information systems has not received due attention. We propose leveraging the NIST model as the underlying methodical guidelines toward incorporating security in the design and development of UHIS. We contend that if security is made a part of the initial design and development process, as proposed by NIST's SDLC, ubiquitous healthcare information systems will be able to become more proactive instead of reactive, while also enhancing the delivery and practice of real-time healthcare that would be trusted by the stakeholders. In order to reap the promised benefits associated with leveraging UHIS, it is imperative for the IS community to tackle the multifaceted aspect of security by conducting future research that can strengthen the strategic role of UHIS in the twenty-first century healthcare delivery and practice.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Ahmed, Z., H. Jamal, R. Mehboob, S. Khan, and M. Shahbaz (2010) "Secure Cognitive Mobile Hotspot", *IEEE Transactions on Consumer Electronics,* (56)2, pp. 606–612.

Bardram, J.E. (2003, October) "Hospitals of the Future—Ubiquitous Computing Support for Medical Work in Hospitals", *Second International Workshop on Ubiquitous Computing*, Seattle, WA.

Baskerville, R. (1993) "Information Systems Security Design Methods: Implications for Information Systems Development", *ACM Computing Surveys* (CSUR), (25)4, pp. 375–414.

Blumenthal, D. (2010) "Launching HIteCH", *New England Journal of Medicine,* (362)5, pp. 382–385.

Bodenreider, O. (2004) "The Unified Medical Language System (UMLS): Integrating Biomedical Terminology", *Nucleic Acids Research,* (32), suppl 1, p. 267.

Bohn, J., F. Gärtner, and H. Vogt (2004) "Dependability Issues of Pervasive Computing in a Healthcare Environment", *Security in Pervasive Computing,* (2802)2004, pp. 160–169.

Borriello, G., V. Stanford, C. Narayanaswami, and W. Menning (2007) "Guest Editors' Introduction Pervasive Computing in Healthcare", *IEEE Pervasive Computing,* (6)1, pp. 17–19.

Brailer, D. (2005) "Interoperability: The Key to the Future Health Care System", *Health Affairs,* (24)5, pp. 1197–1204.

Casalino, L., R.R. Gillies, S.M. Shortell, J.A. Schmittdiel, T. Bodenheimer, J.C. Robinson, T. Rundall, N. Oswald, H. Schauffler, and M.C. Wang (2003) "External Incentives, Information Technology, and Organized Processes to Improve Health Care Quality for Patients with Chronic Diseases", *JAMA: The Journal of the American Medical Association,* (289)4, pp. 434–441.

Chaudhry, B., J. Wang, S. Wu, M. Maglione, W. Mojica, E. Roth, S.C. Morton, and P.G. Shekelle (2006) "Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care", *Annals of Internal Medicine,* (144)10, pp. 742–752.

Cisco (2011) "Cisco 2010 Annual Security Report: Highlighting Global Security Threats and Trends", http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf (current Feb. 1, 2011).

Clark, J.G., N.L. Beebe, K. Williams, and L. Shepherd (2009) "Security and Privacy Governance: Criteria for Systems Design", *Journal of Information Privacy and Security,* (5)4, pp. 3–30.

Cole, L.A. (2000) "Bioterrorism Threats: Learning from Inappropriate Responses", *Journal of Public Health Management and Practice,* (6)4, p. 8.

Coroama, V. and F. Röthenbacher (2003, October) "The Chatty Environment—Providing Everyday Independence to the Visually Impaired", *Proceedings of UbiHealth 2003: The Second International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications,* Seattle, WA.

Da Veiga, A. and J.H.P. Eloff (2007) "An Information Security Governance Framework", *Information Systems Management,* (24)4, pp. 361–372.

Dhillon, G. and G. Torkzadeh (2006) "Value-focused Assessment of Information System Security in Organizations", *Information Systems Journal,* (16)3, pp. 293–314.

Dwivedi, A., R.K. Bali, M.A. Belsis, R.N.G. Naguib, P. Every, and N.S. Nassar (2003, April) "Towards a Practical Healthcare Information Security Model for Healthcare Institutions", *4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine,* Birmingham, UK, pp. 114–117.

Eloff, J. and M. Eloff (2005) "Information Security Architecture", *Computer Fraud & Security,* (2005)11, pp. 10–16.

Epstein, M.A., M.S. Pasieka, W.P. Lord, S.T.C. Wong, and N.J. Mankovich (1998) "Security for the Digital Information Age of Medicine: Issues, Applications, and Implementation", *Journal of Digital Imaging,* (11)1, pp. 33–44.

Farzandipour, M., F. Sadoughi, M. Ahmadi, and I. Karimi (2010) "Security Requirements and Solutions in Electronic Health Records: Lessons Learned from a Comparative Study", *Journal of Medical Systems,* (34)4, pp. 1–14.

Ferranti, J.M., R.C. Musser, K. Kawamoto, and W. Hammond (2006) "The Clinical Document Architecture and the Continuity of Care Record", *Journal of the American Medical Informatics Association,* (13)3, p. 245.

Floerkemeier, C. and F. Siegemund. (2003) "Improving the Effectiveness of Medical Treatment with Pervasive Computing Technologies", *Ubicomp,* Seattle, WA.

Ford, E.W., N. Menachemi, and M.T. Phillips (2006) "Predicting the Adoption of Electronic Health Records by Physicians: When Will Health Care Be Paperless?", *Journal of the American Medical Informatics Association,* (13)1, pp. 106–112.

FPA (2007) "The Privacy Act of 1974", http://www.justice.gov/opcl/privacyact1974.htm (current Jan. 25, 2011).

Giakoumaki, A., K. Perakis, A. Tagaris, and D. Koutsouris (2008) "Digital Watermarking in Telemedicine Applications—Towards Enhanced Data Security and Accessibility", *8th Annual International Conference of the IEEE Engineering in Medicine and Biology Society,* New York, NY, pp. 6328–6331.

Gritzalis, D. and C. Lambrinoudakis (2004) "A Security Architecture for Interconnecting Health Information Systems", *International Journal of Medical Informatics,* (73)3, pp. 305–309.

Grumbach, K. and J.W. Mold (2009) "A Health Care Cooperative Extension Service", *JAMA: The Journal of the American Medical Association,* (301)24, pp. 2589–2591.

Halperin, D., T. Kohno, T. Heydt-Benjamin, K. Fu, and W.H. Maisel (2008) "Security and Privacy for Implantable Medical Devices", *Pervasive Computing* (IEEE), (7)1, pp. 30–39.

Helal, S., C. Giraldo, Y. Kaddoura, C. Lee, H. El Zabadani, and W. Mann (2003, October) "Smart Phone-based Cognitive Assistant", *Proceedings of UbiHealth 2003: The Second International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications,* Seattle, WA.

HIPAA (1996) "Health Insurance Portability and Accountability Act of 1996", http://aspe.hhs.gov/admnsimp/pl104191.htm (current Jan. 26, 2011).

Hoglund, G. and G. McGraw (2004) *Exploiting Software: How to Break Code,* Boston, MA: Pearson Higher Education.

Holden, G. (2003) *Guide to Firewalls and Network Security: Intrusion Detection and VPNs,* Boston, MA: Course Technology Press.

Hu, J. and A.C. Weaver. (2004) "A Dynamic, Context-aware Security Infrastructure for Distributed Healthcare Applications", *Proceedings of the First Workshop on Pervasive Security, Privacy and Trust* (PSPT), Boston, MA.

Hughes, G.F., T. Coughlin, and D.M. Commins (2009) "Disposal of Disk and Tape Data by Secure Sanitization", *Security & Privacy* (IEEE), (7)4, pp. 29–34.

Janczewski, L. and F. Xinli Shi (2002) "Development of Information Security Baselines for Healthcare Information Systems in New Zealand", *Computers & Security,* (21)2, pp. 172–192.

Jepsen, T. (2003) "IT in Healthcare: Progress Report", *IT Professional,* (5)1, pp. 8–14.

Joo-Hak, C. (2008) "Defining the Perfect Ubiquitous Healthcare Information System", http://www.koreaittimes.com/story/defining-perfect-ubiquitous-healthcare-information-system (current Mar. 7, 2012).

Kang, D., K. Kang, H. Lee, E. Ko, and J. Lee (2007) A Systematic Design Tool of Context Aware System for Ubiquitous Healthcare Service in a Smart Home", *Future Generation Communication and Networking,* (FGCN 2007), pp. 49–54.

Kang, D O., H.J. Lee, E.J. Ko, K. Kang, and J. Lee (2006) "A Wearable Context Aware System for Ubiquitous Healthcare", *Engineering in Medicine and Biology Society, 2006, EMBS '06. 28th Annual International Conference of the IEEE,* New York, NY, pp. 5192–5195.

Kara, A. (2002) "Protecting Privacy in Remote-patient Monitoring", *Computer,* (34)5, pp. 24–27.

Kardas, G. and E.T. Tunali (2006) "Design and Implementation of a Smart Card Based Healthcare Information System", *Computer Methods and Programs in Biomedicine,* (81)1, pp. 66–78.

Kawamoto, K. and D.F. Lobach (2007) “Proposal for Fulfilling Strategic Objectives of the US Roadmap for National Action on Decision Support Through a Service-oriented Architecture Leveraging HL7 Services”, *Journal of the American Medical Informatics Association,* (14)2, pp. 146–155.

Khalifa, M. and J. Verner (2002) “Drivers for Software Development Method Usage”, *IEEE Transactions on Engineering Management,* (47)3, pp. 360–369.

Kidd, C., R. Orr, G. Abowd, C. Atkeson, et al. (1999, October) “The Aware Home: A Living Laboratory for Ubiquitous Computing Research”, *COBUILD'99 - Second International Workshop on Cooperative Buildings, Integrating Information, Organizations, and Architecture*, Pittsburgh, PA, pp. 191–198.

Kissel, R., K. Stine, M. Scholl, H. Rossman, et al. (2008) “Security Considerations in the System Development Life Cycle”, *National Institute of Standards and Technology*, http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf (current Feb. 4, 2010).

Kitsios, F., T. Papadopoulos, and S. Angelopoulos (2010) “A Roadmap to the Introduction of Pervasive Information Systems in Healthcare”, in Lazakidou, A., K. Siassiakos, and L. Konstantinos (eds.), *Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications*, Hershey, PA: IGI Global, p. 258.

Kokolakis, S. and C. Lambrinoudakis (2005) “ICT Security Standards for Healthcare Applications”, *Standardization for ICT Security,* (6)3, p. 47.

Korhonen, I., P. Paavilainen, and A. Särelä. (2003a, October) “Application of Ubiquitous Computing Technologies for Support of Independent Living of the Elderly in Real Life Settings”, *UbiComp, Fifth International Conference on Ubiquitous Computing*, Seattle, WA.

Korhonen, I., J. Parkka, and M. Van Gils (2003b) “Health Monitoring in the Home of the Future”, *IEEE Engineering in Medicine and Biology Magazine,* (22)3, pp. 66–73.

Landry, J.P., J.H. Pardue, T. Johnsten, M. Campbell, et al. (2011) “A Threat Tree for Health Information Security and Privacy”, in *Proceedings of the Americas Conference in Information Systems* (*AMCIS) 2011,* Detroit, MI, p. 8.

Le, X.H., S. Lee, Y.K. Lee, H. Lee, et al. (2010) “Activity-oriented Access Control to Ubiquitous Hospital Information and Services”, *Information Sciences,* (180)16, pp. 2979–2990.

Leavitt, N. (2005) “Mobile Phones: The Next Frontier for Hackers?”, *Computer,* (38)4, pp. 20–23.

Leitenberg, M. (2005) *Assessing the Biological Weapons and Bioterrorism Threat*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College.

Liu, L., E. Yu, and J. Mylopoulos (2003) “Security and Privacy Requirements Analysis Within a Social Setting”, *11th IEEE International Conference on Requirements Engineering,* Washington, DC, p. 11.

Liu, Y., J.A. Clark, and S. Stepney (2005) “Devices Are People Too: Using Process Patterns to Elicit Security Requirements in Novel Domains: A Ubiquitous Healthcare Example”, *Security in Pervasive Computing,* (3450) 2005, pp. 31–45.

Matuleviius, R., N. Mayer, H. Mouratidis, E. Dubois, P. Heymans, Z. Bellahsène, and M. Léonard (2008) “Adapting Secure Tropos for Security Risk Management in the Early Phases of Information Systems Development”, in Dubois, E., and K. Pohl (eds.), *Advanced Information Systems Engineering,* New York, NY: Springer, pp. 541–555.

McCallister, E., T. Glance, and K. Scarfone (2010) *Guide to Protecting the Confidentiality of Personally Identifiable Information,* Gaithersburg, MD: DIANE Publishing.

McGraw, G. (2004) “Software Security”, *IEEE Security & Privacy,* (2)2, pp. 80–83.

Mercuri, R. (2004) “The HIPAA-potamus in Health Care Data Security”, *Communications of the ACM,* (47)7, pp. 25–28.

Murphy, S. and H. Chueh (2002) “A Security Architecture for Query Tools Used to Access Large Biomedical Databases”, *Proceedings of the AMIA Symposium*, San Antonio, TX, p. 552.

Mynatt, E.D., I. Essa, and W. Rogers (2000) “Increasing the Opportunities for Aging in Place”, *Proceedings of the 2000 Conference on Universal Usability*, Arlington, VA, pp. 65–71.

Ng, H., M. Sim, and C. Tan (2006) “Security Issues of Wireless Sensor Networks in Healthcare Applications”, *BT Technology Journal,* (24)2, pp. 138–144.

Omary, Z., F. Mtenzi, B. Wu, and C. O’Driscoll (2011) “Ubiquitous Healthcare Information System: Assessment of its Impacts to Patient’s Information”, *International Journal for Information Security Research,* (1)1/2, pp. 71–77.

Page, D. (2010) “A Hospital Imperative: Enterprisewide IT Security”, *Hospitals & Health Networks/AHA,* (84)12, p. 45.

Park, W.S., S.W. Seo, S.S. Son, M.J. Lee, S.H. Kim, E.M. Choi, J.E. Bang, Y.E. Kim, and O.N. Kim (2010) “Analysis of Information Security Management Systems at 5 Domestic Hospitals with More Than 500 Beds”, *Healthcare Informatics Research,* (16)2, pp. 89–99.

Poon, E., A. Jha, M. Christino, M. Honour, R. Fernandopulle, B. Middleton, J. Newhouse, L. Leape, D. Bates, and D. Blumenthal (2006) “Assessing the Level of Healthcare Information Technology Adoption in the United States: A Snapshot”, *BMC Medical Informatics and Decision Making,* (6)1, pp. 1–20.

Rajan, S. and S. Ramaswamy (2010) “On the Need for a Holistic Approach to Information Quality in Healthcare and Medicine”, *Proceedings of the 48th Annual Southeast Regional Conference,* New York, NY, pp. 1–5.

Rindfleisch, T. (1997) “Privacy, Information Technology, and Health Care”, *Communications of the ACM,* (40)8, pp. 92–100.

Shoniregun, C.A., K. Dube, and F. Mtenzi (2010) “Securing e-Healthcare Information”, in Jajodia, S. (ed.) *Electronic Healthcare Information Security,* (53), pp. 1-27.

Smith, J. (2010) “Getting the Right Balance: Information Security and Information Access”, *Legal Information Management,* (10)1, pp. 51–54.

Sneha, S. and U. Varshney (2009) “Enabling Ubiquitous Patient Monitoring: Model, Decision Protocols, Opportunities and Challenges”, *Decision Support Systems,* (46)3, pp. 606–619.

Stanford, V. (2002) “Pervasive Health Care Applications Face Tough Security Challenges”, *IEEE Pervasive Computing,* (1)2, pp. 8–12.

Straub, D.W. and R.J. Welke (1998) “Coping with Systems Risk: Security Planning Models for Management Decision Making”, *MIS Quarterly,* (22)4, pp. 441–469.

Su, Y. and L. Al-Hakim (2010) “Assuring Information Quality in Medical Platform for U-Healthcare Service”, *IEEE International Conference on Wireless Communications, Networking and Information Security,* Beijing, China, pp. 664–668.

Varian, H.R. (2004) “System Reliability and Free Riding”, in Camp, L.J., and S. Lewis (eds.) *Economics of Information Security*, Norwell, MA: Kluwer, p. 250.

Varshney, U. (2003) “Pervasive Healthcare”, *Computer,* (36)12, pp. 138–140.

Venkatasubramanian, K. and S. Gupta. (2006) “Security for Pervasive Health Monitoring Sensor Applications”, *Fourth International Conference on Intelligent Sensing and Information Processing,* Bangalore, India, pp. 197–202.

Venkatasubramanian, K. and S.K.S. Gupta (2007) “Security Solutions for Pervasive Healthcare”, in Xiao, Y. (ed.) *Security in Distributed, Grid, Mobile, and Pervasive Computing*, Boca Raton, FL: Taylor & Francis, pp. 349–366.

Von–Solms, B. (2006) “Information Security—The Fourth Wave”, *Computers & Security,* (25)5, pp. 165–168.

Warren, S., J. Lebak, J. Yao, J. Creekmore, A. Milenkovic, and E. Jovanov (2005) “Interoperability and Security in Wireless Body Area Network Infrastructures”, *27th Annual International Conference of the Engineering in Medicine and Biology Society,* Shanghai, China, pp. 3837–3840.

Weiser, M. (1991) “The Computer for the 21st Century”, *Scientific American,* (265)3, pp. 94–104.

Zafar, H. and J.G. Clark (2009) “Current State of Information Security Research in IS”, *Communications of the Association for Information Systems,* (24) Article 34, pp. 557–596.

Zhang, G. and M. Parashar (2004) “Context-aware Dynamic Access Control for Pervasive Applications”, *Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference,* pp. 219–225.

ABOUT THE AUTHORS

Dr. Humayun Zafar is an Assistant Professor of Information Security and Assurance at Kennesaw State University, Kennesaw, GA. He received his doctorate from the University of Texas at San Antonio. His research interests include organizational security risk management, network security, and organizational performance. Some of his previous work has appeared in journals and conferences such as the *Communications of the Association for Information Systems, Information Resources Management Journal, Journal of Information Privacy and Security, Journal of Emerging Knowledge on Emerging Markets, Human Resource Management Review, Hawaii International Conference on System Sciences,* and *Americas Conference on Information Systems*.

Dr. Sweta Sneha is an Assistant Professor of Information Systems at Kennesaw State University. She received her doctorate in Computer Information Systems from Georgia State University. Her research interests center around a wide array of technical and behavioral challenges related to "E-Health." Within the e-health umbrella, she has conducted and published research in (a) wireless network and enhanced decision support systems for innovative e-health services, (b) adoption, usage, and integration of emerging e-health services in the practice and delivery of healthcare by the healthcare professionals, and (c) organizational impact and process change associated with the integration and usage of e-health services by the healthcare sector. Some of her research has been published in *IEEE Communications, Decision Support Systems, Decision Sciences, International Journal of Medical Informatics, International Journal of Electronic Healthcare, Hawaii International Conference on System Sciences, Americas Conference on Information Systems,* and *IEEE Broadmed*.

Communications of the Association for Information Systems

ISSN: 1529-3181