

# **A Virtual Public Utility for Secure Health Care Transactions**

## **Based on Open Source Software**

**Frederick C. Druseikis, Ph.D.**

Research Associate Professor  
Department of Computer Science & Engineering  
College of Engineering & Information Technology

fredd@engr.sc.edu  
(803) 777 - 2487

**John R. Woods, Ph.D**

Associate Professor  
Department of Family and Preventive Medicine  
School of Medicine  
&  
Director  
Center for Health Services & Policy Research  
Norman J. Arnold School of Public Health

woods@iopa.sc.edu  
(803) 777 - xxxx

Columbia, South Carolina

Version #8 of December 5, 2001

## Project Summary

This research program proposes an open source prototype of a *virtual public utility* for secure health care transactions. We envision the virtual public utility as technical specification fulfilling a number of key design criteria that enables an increased rate of adoption for quantum changes in security infrastructure. We hypothesize that organizations can adopt security innovations faster when approached from a risk management perspective. The design could be instantiated by a *cooperative* of providers, plans, payors, and others in a specific health-economic zone or community. Of central concern to such a virtual public utility would be the common security infrastructure to be provided to the entire health care enterprise. Although public key infrastructure has held a dominant position, there are other possibilities. Such a common infrastructure involves both extensional elements, such as its architecture and technology as manifested in software, as well as intentional elements, such as laws, regulations, rights and traditions fulfilling expectations of groups, organizations, communities, and societies. The development of such a virtual public utility would need to address integration with existing information technologies used in the health care industry, carefully delineating and fulfilling the criteria for sustained use, while attempting to minimize or mitigate the adverse impact of technological change over the entire health care enterprise over a long period of time, possibly measured in decades. Such a public utility could provide benefits in addition to being a least cost implementation of a necessary function in the service of a public good. The object of the research program is to study and model the intrinsically distributed registration authority processes, workflows, and trust models inherent in the health care industry and to demonstrate a prototype of the operation of a virtual public utility that implements those processes in open source software.

## **Project Description**

### ***Introduction***

In this research, we propose to study the following question: How can one increase the rate of diffusion of innovation when the nature of the change is not evolutionary?

Our methodology will be to create a research team to look at the interplay of factors from a software engineering and a risk management perspective. The research team will do primary research in the organizational processes needed to support the societal notions of trust. We intend to build a working model – a prototype – of the virtual public utility concept (discussed below), which will enable specific interactions and expectations to be made clear and demonstrable. Doing so will clarify the nature of technical specifications for this kind of entity. It is beyond the scope of this research to deploy the model or to use it in a specific application setting.

We envision a virtual public utility that enables a group of health care providers, plans, clearing houses, payors, or others to effectively share the cost of providing common infrastructure services and to bear shared risk. To this end we envision the functions of the virtual public utility to be that of transaction routing, security administration, auditing and control. When put into operation, the virtual public utility distributes responsibility for the implementation of common registration authority functions. The users of the utility must trust the actions of other members and jointly assume risk.

We envision the technical specification of the virtual public utility in terms of open source software and the customary artifacts of software engineering. We propose two-year research program to define and create the prototype and its specifications. This will enable the discovery of timely information that will be useful to the health care industry for making decisions over the next five to ten years.

### **Societal Context**

The health care industry in the US is undergoing a process of implementing

mandated federal laws for the use of standards for the use of electronic transactions; see for example, DHHS (2000a). Such transactions are envisioned to take place between different kinds of health care entities – for example, physicians in private practice, hospitals, clinical labs, therapists, and health plans. The integration of technology and the need to innovate are occurring contemporaneously. The concept and justification for “administrative simplification” emerged in the mid 1990’s. It became legislative reality in 1996 with the Health Insurance Portability and Accountability Act; see HIPAA (1996). In a rush to meet the mandate, innovative ideas are in the process of being framed, developed, selected and adopted.

Following Rogers (1995) we can understand the rate of adoption as being determined by such factors as relative advantage, compatibility, complexity, trialability, and observability. Such a model is clearly relevant when adoption proceeds in an *evolutionary* manner with many independent decision makers, and numerous examples of such diffusion of innovation exist. We believe that there are other factors and additional complexities when adoption effects radical or quantum change as would be affected by an organization. Information security frequently demands such *quantum* (non evolutionary) change to infrastructure in the organization.

Security issues for health care are especially sensitive because they intersect with the public policy for privacy of health care information. Rindfleisch (1997) reports on concerns for privacy, information technology, and health care in the era before federal legislation and rule making. In the US, privacy law is in its infancy so the public has little context for deciding the validity or quality of security protections, or even having adequate shared experience for consistently speaking about what such mechanisms mean. In the current day, ordinary language fails us. In this respect, a simple distinction between the intentional semantics of law, policy, politics, civil rights, regulation, tradition, etc., and the extensional semantics of software, architecture, and technology is a simple device for highlighting the issues. But what are the intentions? And whose mechanisms will respect them? Security mechanisms intersect with public policy and organizational policy of a private sector firms. Interestingly, the enacted legislation defines both civil and criminal penalties. Hence, the picture for technology adoption involves *risk management* at the outset as the primary force for making decisions.

Trust and the societal notions of it continue to drive many issues in the practice of information technology. For example, the use of public key infrastructure, described in Dam and Lin (1996), represents a potential approach for certain kinds of authentication processes, which are central to the development of the notion of trust.

### **Open Source Software**

The health care industry in the US is a notorious late-adopter of information technology. Being a late adopter reduces financial risk because it seemingly reduces or eliminates the premiums paid to innovators for their new technology, the very presence of which represents risk until it becomes widely used. The late adoption of technology in practice has left the health care industry in some eyes a bastion of limited or antiquated capability.

Open source software challenges this status quo, because the technology it presents is frequently well known, well understood, and thoroughly vetted through an extensive, highly competitive, if informal, review process. The “gift culture” discussed by Raymond (2001) becomes a source of innovation, but there are alternative views of this process, for example Rugaber and Guzdial (2001). We believe that the process of competitive peer review is a hallmark of the open source process, fed, as it were, by the natural merit accorded to the excellence of a specific implementation, by its design, completeness, or other objective criteria. Adoption in the generic domain of open source software may be explained by other constructs; for example, by a notion of the convergence to an absolute advantage of a series of innovations each demonstrating an incremental relative advantage.

Open source software creates therefore the opportunity to optimize a different set of costs, which are free of the cost of initial capitalization and which are optimally distributed over *all* industries. This renders certain kinds of software components, for example operating systems, compilers, databases, and so forth, commodity items. The cost of developing system becomes one of controlling an integration process, which depends on the quality of interface definitions, as opposed to a software development process, which depends on the quality of functional specifications, component testing, *and* integration.

Open source software therefore presents the prospect of software engineering designs that can endure for decades.

### **The Sharing of Risk**

Although there are risks associated with the adoption of technology itself that can possibly be managed via open source software, the risk management that needs to be addressed involves the standards that will be in place, by which organizations will be held accountable, for the conduct of secure transactions and the sharing of protected information.

Following the analysis of Winn (1999), we recognize that the concept of trust in the law and the concept of trust being articulated in the software industry are potentially discordant. Ellison and Schneier (2000) describe central societal assumptions about the nature of public key infrastructure, a trust that may be misplaced. Forno and Feinbloom (2001) describe a recent incident in which the marketing concept of a public key infrastructure fails to live up to its promise. Winn's analysis points out the legal difficulties with the three-way ("pure") public key infrastructure. Her analysis indicates that the "four-way" model involving a registration authority working with the mechanisms of the certificate authority may be a better solution. So we recognize that fundamental business processes – the registration authority function – need to be trusted in order for privacy to become commonly accepted.

This research proposes to create a prototype for a virtual public utility based on existing standards and interfaces, and to be realized through the use of open source software components. There are several alternative implementations of public key infrastructure in open source. For example, Zurko (1999) describes experiences with an open source implementation created by IBM Corporation and licensed as open source. More recently, Findley (2001) has characterized the state of open source implementations of public key infrastructure. The purpose of the research is to define an example of an information public utility that could securely mediate all of the electronic interactions of providers, plans, and payors in the health care system and address the issues of trust. There may be other paths that should be considered; for example the SDSI PKI proposed by Rivest and Lampson (1996) might have better overall characteristics with respect to

the health care domain. And we should not discount such venerable protocols as Kerberos; see, for example, Neuman and Ts'o (1994). We intend this research to consider these kinds of alternatives. And we intend the research to track the deployment of HIPAA transactions.

### **Key Ideas of this Research**

There are several ideas in this research proposal:

- (1) That there is intrinsic value to a model of a *virtual public utility* instantiated by a cooperative or “co-op” whose services are primarily directed to providing information security for electronic transactions in the health care industry;
- (2) That the modeling of such a virtual public utility, because it so heavily deals with information technology and its *correct* use, is primarily a software engineering research function, which is necessarily well-informed about the needs of the industry through cross-disciplinary collaboration, and which can be best served in an open source model;
- (3) That the mission of the virtual public utility should be to provide the lowest cost implementation of electronic transactions for the public good, in this case the administration of health care services and benefits, and that the central cost minimization issue is one dealing with risk management;
- (4) That there is a critical mass of open source software of sufficient quality to warrant this undertaking;
- (5) That open source software can be used to achieve a cost-effective or optimal implementation of such a public utility; and
- (6) That the existence of cooperatives based on a virtual public utilities of this type would provide a focal point and visibility for accountability of secure electronic transactions in the health care industry, indeed over all of society using the public Internet.

### ***The Notion of the Virtual Public Utility***

We define a *virtual public utility* as a technical specification of a communications infrastructure with certain useful functional behaviors and specific security properties all of which are directed to risk management. The instantiation of the virtual public utility results in an operating entity, which we call a *cooperative*. Our use of the term “virtual public utility” is intended to convey several notions.

The first notion is that there are regulations applicable to the community of members using the operating entity. In this case the regulations have already been stated or are soon to be stated by the Federal Department of Health and Human Services (1998), (2000a), (2000b), and apply to the “covered entities” of the law. The specific objectives for secure health care transactions are well defined and the expectations for security and privacy have been clearly articulated even if not perfectly understood in every instance by all parties. Much discussion has taken place in the industry and is likely to continue unabated for a few more years.

The second notion is that the ownership of the utility is vested in a cooperative owned by a collection of members who each directly benefit from the intrinsic efficiencies provided by the cooperative and who directly bear the expense for operating it. This cooperative ownership (a “co-op”) seeks to minimize costs and share risk in the interests of the members. The co-op might be a not-for-profit corporation whose members proportionately share the expenses of operation.

The third notion is that, because the federal law enabling transactions provides for both civil and criminal penalties, an additional function of the co-op is to indemnify its members in the event that there are violations of the operating rules of utility. Indemnification is a specific requirement needed to assure mutual support of required procedures for registering and authenticating users. These requirements must be supported by the software infrastructure of the utility.

The fourth notion is that the fixed and variable costs for the co-op are governed by specific choices for software engineering choices and processes for organizational development. These choices can be modeled and used to drive software engineering decisions; and conversely, potential software decisions can inform the choices for

organizational development. We think that open source software and standards can drive this process.

The fifth notion is that there is not just one instance of a virtual public utility, just as there is not one electric company, one gas company, or one water company that serves all communities. Health care is almost always delivered locally and there will be certain health-economic zones that naturally lead to the formation of “co-ops”.

The ordinary notion of a public utility often reflects the need for making capital investments that must necessarily be depreciated over long periods, and regulating the prices charged to consumers. For example, nuclear power plants are recognized as being highly capital intensive; and electric power has been seen price regulation for many years. Our term “virtual public utility” construed in this sense of capital intensive is not appropriate here. Clearly the cost of computing equipment is not a significant cost of a virtual public utility (not with Moore’s law still operating.) However the hidden costs of protecting information in health care transactions at the point of breach leads to risk in the form of regulatory judgments with civil, and possibly criminal, penalties. This risk creates the opportunity to share and mutually indemnify owners – who are also users – of the co-op. The risk is created because individual organizations need to adapt to new workflows, significantly different from approaches in the past, and must additionally trust each other according to objective criteria that are not fully defined and not centrally controlled.

### ***The Functions of the Virtual Public Utility***

The health care industry is just beginning to adopt e-commerce transactions into its business processes. Federal law and regulations supporting it now define standards for electronic health care transactions (see DHHS (2000a)) with emphasis on defining privacy rights and obligations to maintain security that have not been mandated before. Many believe that such electronic transactions can improve the efficiency of the health care system by reducing the administrative cost of processing transactions; see, for example, Braithwaite (2001).

The main functions of the virtual public utility we envision are: transaction routing, security administration, auditing and control. Of these, transaction routing, auditing, and control are straightforward.

In defining regulations for privacy and information security, the Department of Health and Human Services has stated a set of generic security requirements; proposed rules for security are stated in DHHS (1998). The cost for an organization to meet these requirements consists of several components, which can be characterized as follows:

- The cost to discover the correct interpretation of the regulations matching the organization's scale and operational style;
- The cost to remediate (i.e., fix) the organization's business practices and information infrastructure to conform to the regulations;
- The cost incurred on an annual basis to maintain correct practice;
- The cost to make future improvements as decided by changes in the regulations from time to time.

The public Internet appears to be a good candidate for implementing a network for health care transactions for several reasons. Probably one of the most compelling reasons is the perceived and actual cost of connecting to the public Internet. Ordinary individuals untrained except for potential first-time guidance from multi-media CD-ROM, printed instructions, or potentially a phone call as last resort, connect to the public Internet – for the first time – daily. But security remains a serious and nontrivial issue. The very scenario of low-cost connection is possibly invalidated by the complexity of

security regulations. Many requirements for information privacy depend on the authentication of users. In its raw form the public Internet fails to provide either of these capabilities in any meaningful form.

The public Internet is often viewed as an “open network.” Open networks are characterized by the ability for new users to join the network without much effort and certainly no central administrative control. The need for trustworthy authentication processes changes that. Much effort has gone into the definition of public key infrastructure, certification authorities, registration authorities, bridge certification authorities, and so forth. In spite of excellent academic credentials PKI still remains a difficult topic.

A PKI is but one approach to solving the *key management problem* for an open network in which there are many millions of potential users. Currently there are many issues with using PKI in the health care system. For example, Winn (1999) identifies certain legal issues with the basic issue of three-way or four-way public key infrastructures. Ellison and Schneier (2000) point out many issues dealing with societal intension for the use of public keys. Key management includes the processes for operating a registration authority, issuing key pairs to valid security principals, assuring access to public keys, and revocation of expired or invalidated keys.

One reason to use a PKI is that allegedly all the problems of key management, once solved in the large, will *scale down* neatly for other kinds of applications. That is, the cost of key management at the scale of the general population of a modern nation state is the least-cost model for solving all key management issues for specific industries at smaller scale. There is a certain appeal to this line of reasoning. This hypothesis is at best untested, and certainly unproven in practice. It contains within it a latent assumption: viz. that all registration processes regardless of application can be implemented at the lowest cost equally well. It ignores, for example, that there might be registration processes that have intrinsically higher costs associated with them and makes the assumption that some kind of linear combination costs distributed over all is acceptable: i.e., that the costs born by one industry can be subsidized by another. This is a problem of “one size fits all.”

The health care industry has several different kinds of registration processes; hospitals engage in “credentialing” of their affiliate medical staffs. Clinical employees are similarly credentialed. Ordinary businesses have their own “human resources” processes. In addition, not-for-profit institutions frequently have a significant volunteer force. All these classes may come into contact with protected health information.

Yet membership in a network supporting health care transactions is fundamentally not open to all; worse, that this notion is possibly a clever dodge for fundamental issues of identity management, which are the processes of binding electronic credentials to individuals. Only valid providers can send legitimate claims to plans and payors. In the terminology of PKI, there would be a registration authority, which would implement business processes to assure that credentials (key pairs) were issued only to legitimate participants. The identity of providers and payors must be well known to each side of the transaction. A valid transaction begins with a legitimate connection to the network, and beyond that arguably begins with network actions that authenticate the end-points before anything is sent. Even in the US, the number of network end-points for a health care transaction network is at a much smaller scale than a PKI is envisioned to operate at, possibly by as much as *three orders of magnitude*.

In short, network end-points, providers and plans, need to trust the processes of the registration authority. But the strength of an open network rests on decentralized administrative processes. Once the registration process becomes decentralized there becomes the problem of how to trust the registrations created by processes that are out of central control. We argue that such central control can never be totally dispensed with; therefore it is an intrinsic cost of doing business that must be managed and distributed amongst all members of the network. A co-op model for sharing expense amongst the participants seems the most natural.

## ***Proposed Research Agenda***

In short the following questions needs to be addressed:

We propose to define cost models that have realistic prospects to support integration, lead to sustainable use within the health care industry and have positive impacts.

We propose to looking across the health care industry as a whole, define and characterize registration authority functions in terms of workflows and to discover the key trust assumptions that must be supported by the virtual public utility. We think this can be done in the context of models for risk management.

We propose to determine one or more models for implementing a registration authority that takes into account the business processes intrinsic to the health care industry.

We propose to analyze the fundamental differences, many of which may be operational, in the choice of different key management technologies. Assuming there were equally viable authentication protocols, such as public key infrastructure, its alternatives, Kerberos, or simply user names and passwords, we would like to characterize what the key management would look like infrastructure that would yield the least cost implementation.

We propose to create technical specifications for the virtual public utility and to demonstrate the concept using open source software. In the course of this we may discover fundamental issues with these implementations that will limit their usefulness – and suggested potential projects that will remedy their deficiencies.

We propose to investigate the diffusion theory of innovation in the context of open source software and in doing so learn how the two relate to each other.

We propose to conduct this research jointly between the Department of Computer Science & Engineering and the Center for Health Services and Policy Research at the University of South Carolina.

## ***Output of the Research***

We envision the following output from this research:

- Full articulation of the concept of the virtual public utility and of the co-op business model assumptions;
- Software engineering artifacts characterizing the virtual public utility;
- Various technical specifications as required to characterize the integration processes;
- A prototype implementation of the virtual public utility for security health care transactions based on open source software;
- Freely available distribution of the prototype;
- Technical Reports, conference proceedings and journal publications.

It is not a goal of this research project to deploy an instance of the virtual public utility.

## References

Braithwaite, William (2001), *Presentation to WEDI HIPAA Summit*, October 25, 2001.  
<http://www.ehcca.com/presentations/HIPAA3/Braithwaite.pdf>

Dam, Kenneth W. and Herbert S. Lin, Eds. (1996) *Cryptography's Role in Securing the Information Society*, Washington DC: National Academy Press.

DHHS (1998), U.S. Department of Health and Human Services, "Administrative Simplification, Security Standards Notice of Proposed Rulemaking," Federal Register 63(165): 43241-43280. August 12, 1998. <http://aspe.hhs.gov/admnsimp/>

DHHS (2000a), U.S. Department of Health and Human Services, "Administrative Simplification, Transaction and Code Set Final Rule," Federal Register, 65(160): 50311-50372. August 17, 2000. <http://aspe.hhs.gov/admnsimp/>

DHHS (2000b), U.S. Department of Health and Human Services, "Administrative Simplification, Privacy Standards Final Rule," Federal Register, 65(250): 82461-82510. December 28, 2000. <http://aspe.hhs.gov/admnsimp/>

Ellison, Carl and Bruce Schneier (2000) "Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure," *Computer Security Journal*, v 16, n 1, 2000, pp. 1-7.

Findlay, Andrew (2001) "Planning for an Open Source Entrant in the PKI Interoperability Trials". <http://www.shirecolts.net/users/david/presentations/skills.pdf>

Forno, Richard and William Feinbloom (2001) "PKI: A Question of Trust and Value," *Communications of the ACM*, 44(6).

HIPAA (1996), Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996," <http://aspe.hhs.gov/admnsimp/pl104191.htm>

Neuman, B. Clifford and Theodore Ts'o (1994) "Kerberos: An Authentication Service for Computer Networks," *IEEE Communications*, 32(9): 33-38.

Rivest, Ron and Butler Lampson (1996), "SDSI: A Simple Distributed Security Infrastructure," available at <http://theory.lcs.mit.edu/~rivest/sdsi11.html>

Raymond, Eric S. (2001) *The Cathedral and the Bazaar*, Sebastopol: O'Reilly & Associates.

Rindfleisch T. (1997) "Privacy, information technology, and health care," *Communications of the ACM* 40(9): 92-100.

Rogers, Everett M. (1995) *Diffusion of Innovations* (4th ed.). New York: The Free Press.

Rugaber, Spencer, and Mark Guzdial (2001) "Ectropic Software," Technical Report, College of Computing, Georgia Institute of Technology.

<http://www.cc.gatech.edu/ectropic/papers/ectropy.pdf>

<http://www.soc.iastate.edu/soc415/soc415.rogers.html>

Winn, Jane Kaufman (1999) "The Hedgehog and The Fox: Distinguishing Public and Private Sector Approaches to Managing Risk for Internet Transactions", *51 ABA Administrative Law Review* 955.

Zurko, Mary Ellen, et. al. (1999) "Jonah: Experience Implementing PKIX Reference Freeware", *Proceedings of the 8th USENIX Security Symposium*, August 23-26, 1999, Washington, D.C.

## ***Principal Investigator – Frederick C. Druseikis***

Dr. Druseikis is Research Associate Professor of Computer Science and Engineering at the University of South Carolina College of Engineering and Information Technology. A computer scientist by training, Dr. Druseikis has spent almost his entire career in the development and application of information technology.

Prior to joining the USC faculty in the fall of 2001, Dr. Druseikis was a co-founder and principal of a South Carolina-based health information technology consultancy, which was subsequently sold. Dr. Druseikis spent over 20 years in the various research and development positions at AT&T/NCR, AT&T Bell Laboratories, the RCA David Sarnoff Research Center, and divisions and subsidiaries of Adventist Health Systems/Sunbelt, where he held various positions as a contributor or manager to advanced development projects that lead to commercial deployment. Prior to his career as an industrial computer scientist, Dr. Druseikis held an academic appointment in the Department of Computer Science at the University of Arizona.

Most recently he held the position as chief software architect for one of the first examples of an Internet-based “first generation” personal health record system (trade-named HealthCompass) build by the former HealthMagic subsidiary of Adventist Health Systems/Sunbelt. This application was first deployed in late 1997 at the Celebration Health clinic operated by Florida Hospital (near Orlando) for residents of the planned community of Celebration, FL. (The town of Celebration, Florida, is a planned community developed by the Walt Disney Company.) Subsequently the HealthCompass application was subsequently marketed to health plans and providers during late 1990’s, and contracted for use by the Internet portal drkoop.com (but not deployed.) The Smithsonian Institution recognized HealthCompass in the Spring 2000 as one example (among several) of the most innovative information technology applications of the 20<sup>th</sup> century.

Dr. Druseikis’ research interests include applications of the public Internet to health care, e-commerce in health care, information security and privacy, and distributed object technology. Dr. Druseikis’ contributions to information technology include the contributions to the development of Object Management Group (OMG) CORBAsec international standards for information security in distributed object systems, and for CORBA interface standards for master-patient indexing systems used in health care.



***Co-Investigator – John R. Woods***

Dr. Woods is Associate Professor of Family and Preventive Medicine at the University of South Carolina School of Medicine, and Director of the Center for Health Services and Policy Research at the Norman J. Arnold School of Public Health. An experimental psychologist by training, Dr. Woods has spent the bulk of his career in clinical and health services research.

Prior to joining the USC faculty in 1998, Dr. Woods spent 21 years at the Methodist Hospital of Indiana, a large teaching and research facility associated with the Indiana University School of Medicine, where he founded and directed the Methodist Center for Health Services Research. He also held an adjunct faculty appointment at the Indiana University School of Public and Environmental Affairs, and was an Affiliate Research Scientist with Indiana University's Bowen Research Institute, an organization dedicated to health services research in primary care and community medicine.

While at Methodist Hospital, Dr. Woods organized and directed the Health Status and Health Risk Survey, a statewide population-based health measurement program sponsored by the North Indiana Conference of the United Methodist Church. He also developed and subsequently directed the Medicare Heart Bypass Demonstration Program at Methodist Hospital, one of six such research and demonstration programs in the United States. In the mid-1980's he participated in the design and analysis of the FDA-supervised trial of the renal lithotripter, an investigational technology designed to treat kidney stones non-invasively using high-pressure shock waves. As a result of this work, he subsequently participated in the NIH Consensus Conference on Kidney Stone Disease, co-authored the first publication analyzing the cost-effectiveness of lithotripsy technology, authored the Report to the Indiana State Board of Health on renal lithotripsy, and co-authored a textbook on emerging technologies in the treatment of kidney stone disease.

Dr. Woods has served as a member or consultant to a number of national organizations, including the Provider Payment Panel of the Health Care Financing Administration Office of Research and Demonstrations, the National Performance Measurement Panel for Coronary Artery Disease sponsored by the Foundation for

Accountability and the U.S. Agency for Health Care Policy and Research, and the Urological National Database Project sponsored by Boston Scientific, Summit Medical Systems and the National Urological Society.

In his current position at the University of South Carolina Dr. Woods serves as a member of USC's Intellectual Property Committee, and is on the Advisory Board of the South Carolina Center for Innovation in Public Mental Health. He is also a consultant to the Palmetto Health Alliance Quality Improvement Coordinating Committee and a member of the Statewide Systems Development Work Group of the Head and Spinal Cord Injury Division of the South Carolina Department of Disabilities and Special Needs.

Dr. Woods' research interests are in the development and use of economic and health status outcome measures, and the use of statistical quality improvement methods in medical care. He is the author or co-author over 60 peer-reviewed journal articles, abstracts, and book chapters.