Claremont Colleges
Scholarship @ Claremont

CGU Faculty Publications and Research

CGU Faculty Scholarship

12-1-2007

An Integrated Social Actor and Service Oriented Architecture (SOA) Approach for Improved Electronic Health Record (EHR) Privacy and Confidentiality in the US National Healthcare Information Network (NHIN)

Gondy Leroy
Claremont Graduate University

Elliot Sloane
Villanova University

Steven Sheetz
Virginia Polytechnic Institute and State University

Recommended Citation

Sloane, Elliot; Leroy, Gondy; and Sheetz, Steven, "An Integrated Social Actor and Service Oriented Architecture (SOA) Approach for Improved Electronic Health Record (EHR) Privacy and Confidentiality in the US National Healthcare Information Network (NHIN)" (2007). AMCIS 2007 Proceedings. Paper 366. http://aisel.aisnet.org/amcis2007/366

This Conference Proceeding is brought to you for free and open access by the CGU Faculty Scholarship at Scholarship @ Claremont. It has been accepted for inclusion in CGU Faculty Publications and Research by an authorized administrator of Scholarship @ Claremont. For more information, please contact scholarship@cuc.claremont.edu.

Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

12-31-2007

An Integrated Social Actor and Service Oriented Architecture (SOA) Approach for Improved Electronic Health Record (EHR) Privacy and Confidentiality in the US National Healthcare Information Network (NHIN)

Elliot Sloane
Villanova School of Business

Gondy Leroy
Claremont Graduate University

Steven Sheetz
Virginia Tech

Follow this and additional works at: http://aisel.aisnet.org/amcis2007

Recommended Citation

Sloane, Elliot; Leroy, Gondy; and Sheetz, Steven, "An Integrated Social Actor and Service Oriented Architecture (SOA) Approach for Improved Electronic Health Record (EHR) Privacy and Confidentiality in the US National Healthcare Information Network (NHIN)" (2007). *AMCIS 2007 Proceedings.* Paper 366.
http://aisel.aisnet.org/amcis2007/366

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2007 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

An Integrated Social Actor and Service Oriented Architecture (SOA) Approach for Improved Electronic Health Record (EHR) Privacy and Confidentiality in the US National Healthcare Information Network (NHIN)

Elliot B. Sloane
Villanova University
ebsloane@villanova.edu

Gondy A. Leroy
Claremont Graduate University
gondy.leroy@cgu.edu

Steven D. Sheetz
Virginia Tech
sheetz@vt.edu

Abstract

The emerging US National Healthcare Information Network (NHIN) will improve healthcare's efficacy, efficiency, and safety. The first-generation NHIN being developed has numerous advantages and limitations. One of the most difficult aspects of today's NHIN is ensuring privacy and confidentiality for personal health data, because family and caregivers have multiple complex legal relationships to a patient. A Social Actor framework is suggested to organize and manage these legal roles, but the Social Actor framework would be very difficult to implement in today's NHIN. Social Actor Security Management could, however, be effectively implemented using Service Oriented Architectures (SOAs), which are rapidly becoming accepted for supporting complex information exchange across heterogeneous information systems fabrics. The Department of Defense is applying SOA to all of its enterprises. It is using customized simulation and modeling tools to achieve security and robustness goals and to reduce the intrinsic design and implementation risks for SOA's complex Systems of Systems environment. This paper integrates all of these approaches into a next-generation NHIN-2 design based on a specific Air Force SOA named MCSOA. This NHIN-2 design uses MCSOA to create Security Management, Service Discovery, and Presence Management agents to implement Social Actor support for improved confidentiality and privacy.

Introduction

In the United States, the delivery of healthcare is complicated by the numerous factual, functional, and legal roles that individuals can have in the US healthcare delivery system. This paper explores the complexity of developing a user-centric Electronic Health Record (EHR) system for the National Healthcare Information Network (NHIN) that is currently under development by the US Department of Health and Humans Services (DHHS). In particular, we discuss the advantages of designing the system using the concept "social actors," instead of specific users, in order to match complex healthcare needs. Further, the advantages of ultimately employing a Service Oriented Architecture (SOA) design for NHIN that could be patterned after the net-centric initiatives Department of Defense (DoD). An SOA approach would allow more efficient, cost-effective, and flexible design, implementation, and support of the NHIN.

This paper has three main parts: 1) an explanation of the advantages and risks of the NHIN, and its Regional Healthcare Information Organization architecture; 2) a discussion of an enhanced-SOA system under development for the Air Force, ; 3) a brief explanation of how Villanova's modeling and simulation tools help assure DoD that the complex System of Systems it is designing will work properly; and 4) how these DoD systems can be used to design a next-generation NHIN-2 The paper concludes with a discussion about potential next steps for NHIN-2.

Users as Social Actors

As will be described in shortly, two fundamental goals of the NHIN are to 1) enable "consumer empowerment," to help the US public consumer make better-informed healthcare decisions, and 2) create Electronic Health Records (EHRs) for all consumers by 2014 to support their decisions and to improve the quality, quantity, and completeness of information available to physicians. Although the patient is indeed the source of whatever relevant clinical tests and data belong in the EHR, in many situations that individual may not able to directly evaluate, interpret, or make decisions from information available in the EHR.

In the healthcare world, the security needs are quite demanding due to the rigorous and often divergent Federal and State HIPAA requirements. For example, Massachusetts has specific HIPAA disclosure data restrictions for HIV tests and drugs that may differ from other states (Massachusetts 2006). The Massachusetts law must be obeyed for data that in or out of any system in that state. This only one of hundred of specific privacy rules created at state and federal levels.

Each state and personal health situation may carry multiple unique privacy and security obligations, and, unfortunately, we cannot simply apply a single simple rule to control access to data. If we consider a single disease like diabetes, we can get a sense of the richness and complexity of this challenge for a comatose diabetic patient in a hospital's Emergency Department setting.

If, for example, a patient is a child, the biological parent of a childwith Type 1 diabetes might be expected to act as the legal surrogate for the child's medical care and would nominally be the individual with authority to view and act on information in the EHR. This is not always the case, however. For example, if the child is in foster care, the court may have appointed an independent legal healthcare surrogate, or if the child has been adopted, the adoptive parents would have that authority. Even if one or more biologic or adoptive parents nominally are the legal surrogates, other situations such as parental incapacity or death, or court intervention due to child abuse, may temporarily over-ride the nominal legal authority. In such cases, depending on the situation the court, a statement of custodial care in a parent's will, or a next-of-kin may have the right and obligation to assume the role of legal surrogate. The situation also gets more challenging as the patient nears the age of majority, typically at 18 years old, because as soon as that birthday is passed, the patient now assumes legal authority for decisions and data access. Finally, if the patient happened to be married before turning 18, their spouse may well have legal authority to see and act on information in the EHR, though it is conceivable that a parent still bears the insurance and payment responsibilities.

If the patient is an elder adult, the problem can be just as complex, or more so, considering state law complexities. Legal authority for access and use of the EHR may depend on marital or life partner status, competency of the living spouse or life partner, various legal power of attorney documents held by children or friends, and even court injunctions that affect the situation.

These situations are made even more complex if the patient is also an employee, or relative of an employee, of the hospital where they are treated, which is not an unusual situation. In a rural setting with only one hospital it is even possible for the surgeon to treat a relative such as a spouse or a child. Though that surgeon may be reasonably entitled to much patient data related to their immediate care, they may not be entitled to unlimited access to confidential psychiatric, gynecologic, or pharmaceutical data.

The complexity of the actual situations encountered in healthcare makes it very difficult to actually design and develop a simple patient- or user-centric EHR system. The authors suggest adopting a more flexible framework that labels users as complex "social actors." The Social Actor concept was created to describe widely varying Affiliations, Environments, Interactions, and Identities for computer system users (Lamb and Kling 2003). In the social actor framework, one or more of the decision makers in the earlier examples would be placed into an Affiliation labeled "legal guardian with power of attorney," while another person's Affiliation might be labeled "family member with approved access to the EHR." The Environment attribute might be useful to precisely define each individual's authority in different hospital settings, such as the Emergency Department, Intensive Care Unit, or Rehabilitation. The Interactions attribute might be useful to segregate "information access only" from decision or financial responsibilities, while the Identities attribute might be used to clarify the heredity, legal, employment, clinical care role, or other relationship.

None of the complexities discussed above are really restricted to diabetes, but are shared by any other situation involving life-threatening disease or traumatic injury, and the National Healthcare Information Network must be able to provide an appropriate balance of privacy, efficiency and efficacy in order to succeed.

The National Healthcare Information Network (NHIN)

In 2004, President Bush authorized the US DHHS to initiate the design and development of a first generation National Healthcare Information Network (Bush 2004). NHIN by nature is a complex System of Systems Engineering (SoSE) challenge because contemporary healthcare depends on multiple disparate clinical specialists (e.g., radiologist, cardiologist, or rheumatologist) and care-delivery-providers (e.g., hospital, physician office, or home care), each using specialized computer systems for optimal clinical data and practice management (Sloane, et al. 2007). In addition, telemedicine tools are creating an ever-expanding diversity of points-of-care, creating a growing number of smaller healthcare subsystems that extend to personal, consumer-based health care technologies.

A primary goal of the NHIN is to create Electronic Health Records (EHRs) for all citizens by 2014. The EHR is not simply an administrative nicety: It is seen as a critical means to eliminate the disparate silos of computer- and paper-based patient records. The inability for physicians or patients to obtain complete, up-to-date clinical data has been identified as a critical gap in healthcare, which must be eliminated in order to recover 30-40% of wasted annual healthcare expenditures caused by duplicated and erroneous processes (NAE/IOM 2005). In addition, incomplete EHRs and inability of physicians to obtain correct and current clinical information causes tens of thousands of needless annual serious patient injuries and deaths believed caused by medical errors such as drug mistakes in the US (IOM 2000).

In 2005 and 2006, the Department of Health and Human Services actually began the design and development of their first-generation NHIN (ONCHIT 2006). The initial three requirements placed on NHIN were to: 1) create a technical framework to allow complete and timely sharing of medical data between physicians, 2) create the foundations of an Electronic Health Record (EHR), and 3) empower consumer decision-making by making their EHR available to them. To focus this work, only two high-interest medical categories were identified for implementation: chronic healthcare diseases, which have the highest costs and affect the most vulnerable patients, and biosurveillance, to help manage the risk of potential pandemics like SARS or avian flu. The NHIN features that were selected for the implementation each year were selected by teams of clinicians, providers, and researchers who were organized into panels within a new American Healthcare Information Community (AHIC), which report directly to ONCHIT (AHIC 2007).

A critical success factor of NHIN is information and information system interoperability, to ensure that relevant medical tests and clinical findings can be reliably and securely relayed wherever patient treatment is taking place. The NHIN project development process employs an iterative, one-year analysis-design-prototype cycle of systems design and testing. Essentially, once AHIC has specified the coming year's NHIN goals, another DHHS-funded group known as the Healthcare Information Technology Standards Panel (HITSP) identifies, evaluates, and recommends the most appropriate technical frameworks and standards that DHHS should specify in order to meet the interoperability and EHR goals specified by AHIC (HITSP 2007). The first round of HITSP recommendations were finalized in late October, 2006, and they were accepted by the Secretary of Health in January of 2007 (DHHS 2007). Those recommendations are now being used to support development and implementation of pilot Regional Healthcare Information Organizations (RHIOs) in 2007, as described below.

Regional Healthcare Information Organization (RHIOs), the Initial Architecture of the NHIN

It is worth noting that by regardless of configuration, the NHIN is a complex System of Systems (SoS) challenge because contemporary healthcare depends on multiple disparate clinical specialists (e.g., radiologist, cardiologist, or rheumatologist) and care-delivery-providers (e.g., hospital, physician office, or home care). Each specialist has unique proprietary computer systems for optimal clinical data and practice management. In addition, telemedicine and personal health devices are enabling an ever-expanding diversity of points-of-care, creating a growing number of smaller healthcare subsystems that extend to rural and personal, consumer-based health care technologies (Continua 2007, Pearce 2002). The SoS nature of healthcare information system creates unique challenges for the NHIN, because it would be extremely complicated to connect over 100,000 systems used by physicians and hospitals. In fact, to connect N different computer systems would require nearly N(N-1), or roughly N^2 interfaces between all of the systems! Such a complex SoS would not only be expensive to create, but would also have N^2 points of failure or security breach, which is unacceptable.

Further, because the US does not have a single public health system, ONCHIT did not believe creating a central national medical data warehouse for all citizens' data, or requiring all healthcare providers to replace their computer systems with a single homogeneous design, were feasible alternatives. Instead, during 2007 four teams of vendors and providers have been funded by DHHS to build and test demonstration pilot projects for a nationwide hub-and-spoke networked system of Regional Healthcare Information Organizations (RHIOs). Each of these four custom-built RHIOs serve as computing and communication hubs that convert legacy system data from partner hospitals and physician offices and transfer that data to/from the other pilot RHIOs.

To illustrate how the RHIOs should function, we might consider what would happen if a patient from Philadelphia was injured while skiing in Utah. The RHIO in Utah would locate all available medical data for that patient through a RHIO near Philadelphia and transfer it to Utah. The Philadelphia RHIO's job, though, is not specifically to maintain all of the data in a region. Instead, it serves as a central registry and data collection, transformation, and relay system for all of the patient data held by its hospital and physician members. The HITSP frameworks and standards essentially govern the transfer of data between the RHIOs, leaving the RHIOs and their members some latitude in deciding their own internal systems, software, and standards.

Advantages of the Initial RHIO Architecture

This RHIO architecture has many advantages, including the following:

- Most patient data is kept in the hospital, specialty departments, and physician offices the patient visits most frequently, ensuring rapid availability for the most likely clinical users, the patients, and their families.
- Each RHIO may be flexibly designed to support a finite variety of local legacy healthcare information systems instead of having to simultaneously support all potential legacy systems across the country;

- Any single RHIO or telecommunication failure should be a local event that is unlikely to disrupt patient care in other regions;
- Confidential, life-critical patient data is not aggregated in any single repository where it could be vulnerable to privacy breaches, tampering, or loss;
- The emerging HITSP standards that have been accepted by the Secretary of Health are based on commonly-accepted XML data formats, which help ensure ready data identification and interpretation; and
- The NHIN's RHIO architecture is based on a PULL data model, whereby RHIOs responses can be limited to patient inquiries it receives.

Challenges and Risks of the Initial RHIO Architecture

The RHIO architecture currently moving into pilot and demonstration phases can be visualized as a national network of proprietary regional star networks that are designed to facilitate relatively 'static' data transfers between local and regional providers. This RHIO architecture has several fundamental risks, including:

- Lack of RHIO standardization could lead to extensive continuous, expensive, and error-prone maintenance of each proprietary RHIO to match expanding clinical and technical requirements;
- Reactive data and software management among RHIOs is likely, unless each RHIO aggressively monitors and incorporates the inherently dynamic volume and type of medical information it must handle;
- Though a single point RHIO failure may not affect other regions, it could cause major expensive or life-threatening disruptions *within* its own region, precisely where most covered patients will seek medical care;
- If one or more RHIOs introduces significant information gaps or capacity constraints into the national RHIO network because of operational, financial, or technical difficulties, that could have expensive or life-threatening regional/national consequences for patients and providers;
- Patients who live near two or more RHIO fringe areas are likely to constantly have clinical records spread among two, three, or more RHIOs;
- Physicians and hospitals that change outsource providers for laboratory, imaging, or other services may similarly select outsource resources that span multiple RHIOS;
- No national patient identifier exists, so all RHIOs will need to depend on each others' implementation of statistical matching tools based on available patient demographic data;
- If any of the RHIO communication links fail, there may be no way to detect the failure and/or restore that connection when the problem is fixed;
- Because the RHIOs and individual hospitals comprises a complex System of Systems, it is difficult, if not impossible, to predict the effect of changes or failures of one or more systems or components;
- Newly acquired patient data, such as the recall of a drug dispensed by the patient's "home" hospital, may not be forwarded to the remote RHIO unless it happens to request new updates; and
- Since patient data can only be provided to parties with legal authority for access, each RHIO and individual system will need to create and manage its own robust and complex authentication systems to control access.

SOA Enhancements for the Department of Defense

In order to lay the necessary foundation for the remainder of our paper, we now present a summary of Villanova's recent Advanced Research for Computing Enterprise Research (ARCES) work for the Air Force (see Acknowledgements in the last section below). This work is helping DoD design and deploy their enhanced Service-Oriented Architecture (SOA), which has unique robustness and security requirements. We believe that this enhanced-SOA system offer a promising direction for a next generation NHIN, which we have called NHIN-2 (Sloane, et al. 2007)

As shown in Figure 1, SOA is a distributed network architecture design approach that partitions service providers (or provision) from service consumers (or consumption), using service brokers to manage the process.

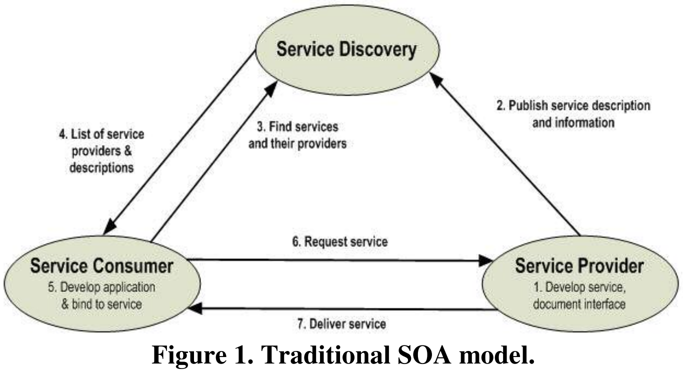
Service Discovery
4. List of service providers & descriptions
3. Find services and their providers
2. Publish service description and information
6. Request service
Service Consumer
5. Develop application & bind to service
Service Provider
1. Develop service, document interface
7. Deliver service

Figure 1. Traditional SOA model.

Self-contained services communicate with each other when required, yet they do not depend on the state of other services, creating a loosely coupled architecture that is easily reconfigurable. The SOA approach is attractive for complex System of Systems (SoS) designs because of its flexibility and reusability, and its isolation of functionality from the details of implementation. The roles commonly described in SOA are Service Provider, Service Consumer and Service Broker. The Service Provider offers services, making them available by publishing service interfaces in a Service Registry. The Service Consumer uses Service Provider services based on published service interface rules. The Service Broker component manages the registry for both Providers and Consumers.

In the "traditional" SOA model, the available Service Provider services are often static. For example, a single-hospital SOA could use the hospital's Admission/Discharge/Transfer (ADT) system as their Patient Registry SP, which users might query for patient names, addresses, and other demographic and billing data. The elegance of the SOA architecture is that any new Service Consumer, like a hospital's new homecare business, could plug into SOA immediately to help manage its homecare activities. Any new Service Consumer only has to create a single interface to the hospital's SOA system, following the hospital's SOA communication and data protocols.

The flexibility and 'plug-and-play' interoperability of SOA led to its adoption by DoD for all of its enterprise services. The DoD and Defense Information Systems Agency (DISA) have defined a core set of services for defense-related SOA systems in its Net-Centric Enterprise Solutions for Interoperability (NESI) initiative (NESI 2007).

The Net-Centric Enterprise Services defined by NESI include services, nodes and utilities for use in DoD domain, and mission-related enterprise information systems, and have led to significant, ongoing development efforts. Many key SOA requirements for DoD are shown in Table 1.

Table 1. Key SOA requirements for DoD

• Service guarantees • Fault tolerance • Load balancing • Interoperable multiple connection types	• Security • Dynamic service discovery • Availability awareness (a.k.a. "presence management")

These three examples of challenges and solutions for DoD's SOA requirements help illustrate the differences from "traditional" static SOA implementation:

1. **Security:** An officer's PDA may allow her to pull up combat-related maps and even send IM feedback to her subordinates. That officer may have extensive access to high-security-clearance data and personnel, but if the PDA falls into a civilian's hands, the access to sensitive data at potentially hundreds of military Service Providers within the DoD's SOA fabric must be abruptly and effectively cut off. A very robust and dynamic Security Manager is necessary for DoD SOA deployments.
2. **Dynamic service discovery:** If a new GIS-based Improvised Explosive Device (IED) database were suddenly created, all service personnel's PDAs would certainly benefit from access to that data immediately. In the "classical" SOA context, all of the Service Consumer modules in all PDA's, and the main Service Broker itself, may need to be updated with software patches to allow access to the new IED SP. For DoD applications, a robust and dynamic Service Discovery module could work with the Service Broker to automatically handle these demands seamlessly.
3. **Availability awareness:** If the IED Service Provider is maintained in an on-position AWACs airplane, communications with multiple officers' PDAs can be expected to drop offline periodically. In "traditional" SOA, the general expectation is that fairly robust continuous network and/or Internet access remains in an "always-on" state. For DoD applications, a Presence Management module could work with the Security Management and Service Discovery modules to ensure that when any PDA comes back online, it is a) authenticated for access to secure data and personnel, b), provided immediate status updates from the Service Providers it had been using, and c) notified of any new services that had been added.

There may be multiple ways to achieve the SOA robustness and flexibility that DoD requires. One that is under development for Wright Patterson Air Force Base is called the Multi-Channel Service Oriented Architecture (MCSOA) (Gestalt 2007).

A key enhancement goal of MCSOA is the Dynamic Service Discovery Agent (DSDA) shown in Figure 3. Depending on configuration, the DSDA can handle any or all of the enhanced tasks listed in Table 1. In fact, the DSDA's must also exhibit sufficient redundancy that full or partial failure of any single Agent can be overcome by one or more available Agents. The MCSOA simulation, modeling, and development process includes the Security Management, Service Discovery, and Presence Management tasks described above.

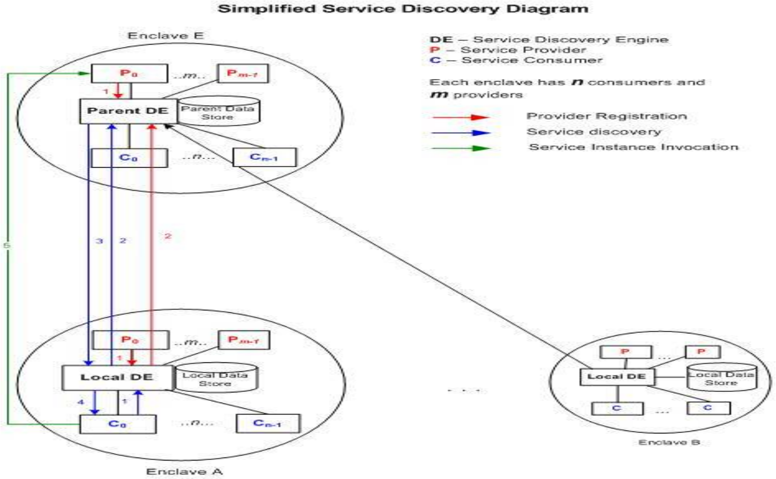

Figure 2. MCSOA Dynamic Service Discovery Agent

DoD's SOA implementation is a complex System of Systems, and cannot simply be assembled and tested without huge risks and expense. DoD requires simulation and modeling be used throughout the design and testing of complex SoS projects to discover operational boundaries and optimization strategies for alternate system designs. Villanova's ARCES project uses a freely available "formal methods" simulation tool known as the Colored Petri Net (CPN), and a second, hybrid proprietary discrete simulation tool known as MESA/Extend to do whitebox and blackbox simulations and modeling. Details on the simulation, modeling, and design of these SOA enhancements have been published elsewhere, and are not repeated here (Sloane, et al 2007).

Proposed Enhanced-SOA NHIN-2

We will now use the above three DOD SOA use cases to illustrate how to create an acceptable enhanced-SOA NHIN-2. The following three NHIN-2 use cases parallel the DoD examples:

1. **Security:** To meet state-specific HIPAA laws using MCSOA, a central "HIPAA Service Provider" can be created that maintains all of the State and Federal HIPAA privacy laws and exceptions. Another "Social Actor Service Provider" could contain all authenticated physicians, nurses, family members, court surrogates, or other people, along with the complex set of laws and guidelines that dictate what data they should see at any moment in time. A Security Manager tool that integrates HIPAA and Social Actor roles for all healthcare applications could also be created. This resource would obviously be quite complex, but making this service available to all RHIOs as a SOA resource would improve security, avoid mistakes, and reduce costs for everyone.

2. **Dynamic service discovery:** Medication errors cause tens of thousands of annual deaths in the US (IOM 2000), and manufacturers periodically recall individual batches/lots of drugs, or identify new dangerous drug interactions, or both. If new dangerous drug information that affects an individual patient becomes available, MCSOA's presence and discovery tools could broadcast that information to any hospital treating a patient immediately.

3. **Availability awareness:** The two above use cases can be generalized to illustrate the role MCSOA's Presence Manager fills. For example if a "first responder" such as an EMT was attempting to revive a non-responsive traffic accident victim in an ambulance, the wireless link to the ambulance might be quite erratic, especially when tunnels, mountains, or thunderstorms are encountered. If data about the victim's medications or diabetes status comes available during a periodic communications lapse, the Presence Manager would store and forward that critical data as soon as the wireless link was re-established.

Conclusions

We have proposed leveraging emerging DoD research and development as a valuable "dual use" or "peacetime dividend" for the US national healthcare infrastructure. The MCSOA system under developed for DoD includes Security Management, Service Discovery, and Presence Management capabilities using Dynamic Service Discovery Agents. These features could be used in NHIN-2 to improve individual and aggregate static data exchange between RHIOs in many ways. For example, the Security Manager, Service Discovery, and Presence Management features can be used together to help guarantee automatic updates to all bona fide healthcare providers to protect and improve a patient's care. The Service Discovery mechanism, integrated with Presence Manager support, ensures up-to-date data by observing and posting updates as part of its registration/presence information.

Using Villanova's DoD presence and discovery modeling tools, the proposed NHIN-2 can also improve context-awareness and fault-tolerance in tasks such as managing a telemedicine application's bandwidth constraints by automatically compressing data, or applying dynamic load-balance in a heavily loaded system to reduce system faults. Building systems based on the conceptual NHIN-2 model, even as prototypes can be prohibitively expensive. By leveraging the CPN and MESA/Extend MCSOA modeling techniques we developed for DoD, our models can be used to confirm that NHIN-2 system designs and configurations have the expected and desirable properties, and to gain new insights into the workings of the system. This approach avoids wasted programming or resource deployment by detecting and fixing robustness, security, flexibility, safety, or reliability faults early in the design and configuration process.

Acknowledgements

Villanova's Advanced Research for Computing Enterprise Services (ARCES) project was supported in part by the Air Force Materiel Command (AFMC), Electronic Systems Group (ESG) under contract number FA8726-05-C-0008. The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of USAF, AFMC, ESC, or the U.S. Government.

References

AHIC Workgroups web site at U.S. Department of Health & Human Services, Health Information Technology. Last accessed at: www.hhs.gov/healthit/ahic/workgroups.html on April 29, 2007.

Bush, G. W. "Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator," Executive Order 13335 of the President of the United States, 31 April, 2004.

Continua Health Alliance web site. Last accessed at: www.continuaalliance.org on 29 April, 2007.

DHHS (Department of Health and Human Services) "Secretary of Health Acceptance and Planned Recognition of Certain Healthcare Information Technology Standards Panel (HITSP), Interoperability Specifications for Health Information Technology," US Federal Register, March 1, 2007. 72(40) p. 9339.

HITSP (Healthcare Information Technology Standards Panel) web site, American National Standards Institute (ANSI). Last accessed at: www.ansi.org/hitsp on April 29, 2007.

IOM (Institute of Medicine). "To Err is Human: Building a Safer Health System," National Academy Press, 2000. Washington, D.C. Available at: http://www.nap.edu/

Gestalt, LLC. "Service-deployment frameworks and routing fabrics: the elements of a multi-channel service oriented architecture (MCSOA).\," Whitepaper, available at: http://www.gestalt-llc.com/resources/d_mcsoa.pdf, last accessed on 29 April, 2007.

Lamb, R. and Kling, R. "Reconceptualizing Users as Social Actors in Information Systems Research," MIS Quarterly, (27:3) June 2003, pp. 197-235.

Massachusetts Bureau of Communicable Disease Control: Frequently Asked Questions Regarding Reporting of Communicable Disease under HIPAA web site. Last accessed at: http://www.mass.gov/ dph/comm/hipaa/faq_cdc.htm on 29 April, 2007.

NAE/IOM (National Academies of Engineering and Institute of Medicine joint report). "Building a Better Delivery System: A New Engineering/Health Partnership," National Academy Press, 2005. Washington, D.C. Available at: http://www.nap.edu/.

NESI (Netcentric Enterprise Solutions for Interoperability) public web site, U.S. Navy. Last accessed at: http://nesipublic.spawar.navy.mil on 29 April, 2007.

ONCHIT (Office of the National Coordinator for Health Information Technology) Health Information Technology web site, U.S. Department of Health & Human Services. Last accessed at: www.HHS.gov/healthit/ on April 29, 2007.

Pearce, F.W. "The Alaska telemedicine testbed project (1996-2001): digital healthcare in a narrow bandwidth environment," Proceedings of the 2002 annual national conference on Digital government research ACM International Conference Proceeding Series; Vol. 129. pp 1-51.

Sloane, E., Way, T., Gehlot, V., Beck, R., Solderitch, J. and Dziembowski, E. "SoSE Modeling and Simulation Approaches to Evaluate Security and Performance Limitations of a Next Generation National Healthcare Information Network (NHIN-2)," IEEE Systems Council and Systems, Man, and Cybernetics Society: Proceedings of the International Conference on System of Systems Engineering, San Antonio, TX. 16-18 April, 2007 (In production).

Sloane, E., Way, T., Gehlot, V., Beck, R. "Conceptual SoS Model And Simulation Systems For A Next Generation National Healthcare Information Network (NHIN-2): Creating A Net-Centric, Extensible, Context Aware, Dynamic Discovery Framework For Robust, Secure, Flexible, Safe, And Reliable Healthcare," Proceedings of the 1st Annual IEEE System of Systems Conference, Honolulu, Hawaii. 9-12 April, 2007 (In production).

Sloane, E.B., Way, T., Gehlot, V., Beck, R., Solderitch, J., Dziembowski, E. "A hybrid approach to modeling SOA Systems of Systems using CPN and MESA/Extend," Proceedings of the 1st Annual IEEE Systems Conference, Honolulu, HI, April 9-12, 2007.