R. S. Raman, V. Jagannathan, K. Srinivas, S. Reddy, K.J. Cleetus, R. Reddy

Concurrent Engineering Research Center,
West Virginia University,
Morgantown, USA.

Review Paper

Collaboration Technology for Rural Health-care

Abstract: Health-care is a collaborative endeavor involving a number of individuals and organizations with diverse perspectives. Computer-supported collaboration technologies have great potential to enable health-care providers to improve the quality of care provided to their patients. Such technologies have the potential to overcome barriers to quality health-care in the small, scattered populations of rural areas. Rapid changes in technology are making it more and more possible for collaborative telemedicine to be a part of the practice of medicine. The World Wide Web has amply demonstrated that the globe has shrunk and information from afar is a mere mouse click away. However, the ease with which information is accessed along with the potential disclosure and misuse of personal information has raised serious concerns about the ability to restrict such information to legitimate accesses by duly authorized health-care providers. The authors present their experience in developing a health-care collaboration facility, ARTEMIS, which enabled Web-based access to electronic medical records, and provide a vision of their experiment to provide secure telemedicine for rural health-care practitioners.

Keywords: Telemedicine, Computer-based Patient Records, Confidentiality of Electronic Health Information, Collaboration Technology.

Introduction

"Telemedicine gives doctors a second opinion. In seconds." reads the caption of a Wall Street Journal advertisement by Europe's leading telecommunications company, Deutsche Telekom. Clearly telemedicine has captured the imagination of many people and organizations with many viewing telemedicine as a panacea for improving access to health-care while reducing costs. According to a recent article in Telemedicine Journal,

"Telemedicine is the use of modern telecommunications and information technologies for the provision of clinical care to individuals at a distance and the transmission of information to provide that care. It includes diagnosis, treatment, monitoring and education of patients using a system that allows ready access to expert advice and patient information no matter where the patient or relevant information is located."

From this perspective, telemedicine goes far beyond merely the means to quickly get a second opinion or a remote consultation — it can empower a patient to actively participate in the health-care delivery process and its outcome. Furthermore, by enabling a patient to receive care at, or close to, home, it allows all of the patient's support network (family, neighbors and friends) to work in concert with traditional caregivers, resulting in an improvement of the quality of care provided as well as a reduction of the direct and indirect costs of health-care delivery.

Patient centered health-care delivery is an inherently collaborative process involving a wide range of individuals and organizations with diverse perspectives. The patient receives care from a combination of players — individual physicians, a physician group or a health-care institution. Their health-care delivery activities, in turn, are influenced by payers, national information resources such as the National Library of Medicine (NLM) and research establishments such as the Centers for Disease Control (CDC). Together, all participants collaborate, explicitly or implicitly, to deliver quality care at a reasonable cost.

Evolution of Telemedicine Frameworks

The technology available for telemedicine may be classified into a series of generations (Fig. 1). The first generation of telemedicine only supported the fax as the means of data transmission, thus the only infrastructure needed was phone lines. The second generation introduced satellites and private networks using leased lines to transmit analog video, permitting "face-to-face" consultation electronically using video-conferencing technology. The third generation began with the Internet era. Pieces of the patient record were electronically available and, more recently, desktop conferencing systems have become available. The fourth generation will be characterized by the integration of real time monitoring systems into the electronic patient record and by the availability of groupware for decision support. Finally, generation five will encompass the ubiquitous World Wide Web, secure communications on the Internet, object exchange mechanisms such as CORBA and OLE, and the integration of the patient record (the product) with the workflow (the process).

Quite a few organizations, including that of the authors, have built and demonstrated working prototypes of telemedicine systems. While some of these systems show considerable promise, all are far from realizing their full potential until several fundamental barriers are overcome by:

1. assuring privacy and integrity of medical information stored in computers and during communication over public networks.
2. seamlessly integrating telemedicine applications into the "workflow" of health-care providers.
3. providing a standards-based, open architecture to enable the creation of plug-and-play component based solutions which can access information from legacy systems.
4. demonstrating cost-effectiveness measures by migrating research prototypes into real-world operational environments.

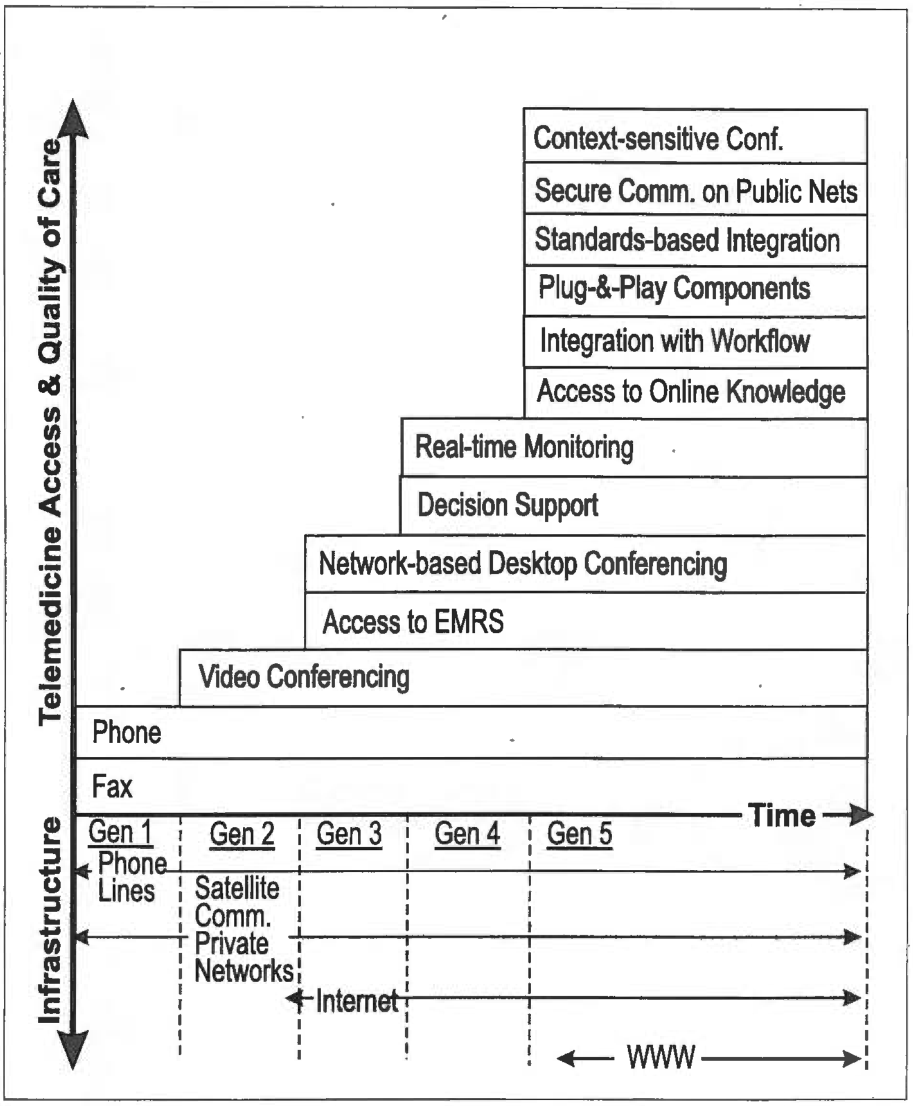

Figure 1. Evolution of telemedicine.

Confidentiality of Electronic Health Information

The advent of computer-based patient records, the increasing penetration of computers into the businesses and homes of health-care providers and the fast growth of electronic mail and Internet-based applications and resources such as the World Wide Web have fostered the hopes of collaboration among health-care providers who may be geographically apart. However, concerns about the security of electronic medical information, its interception and modification during transmission via the Internet, and the opportunities through aggregation for the misuse of personally identifiable health-care records, have kept many from participating in collaborative health-care delivery. Encryption facilities are slowly being introduced into applications and servers, showing promise that reasonably secure business transactions may soon be safely conducted through computers on the Internet. Given the sensitivity of patient records and the possible litigious reactions, health-care providers have taken a wait-and-see attitude to adopting computer-based collaboration facilities and telemedicine.

These observations are in line with the preliminary findings of the United States' National Research Council's

Computer Science and Telecommunications Board's study on the privacy and security of health-care information. They found that some of the risks for electronic health information include:

- improper or inadvertent disclosure of sensitive information by privileged health-care providers
- unauthorized access to health-care information by persons taking advantage of inadequate protective measures to computer and communication systems and repositories
- insidious use of computer database aggregation and inferential analysis to identify individuals, using correlation to other known characteristics
- unauthorized alterations and modifications due to inadequate measures for ensuring the authenticity and data integrity of electronic health information.

These risks can be addressed through a combination of technical, organizational and legislative measures that protect the confidentiality and integrity of electronic health information (Fig. 2). Below is a partial list of measures for dealing with the data security issues in telemedicine.

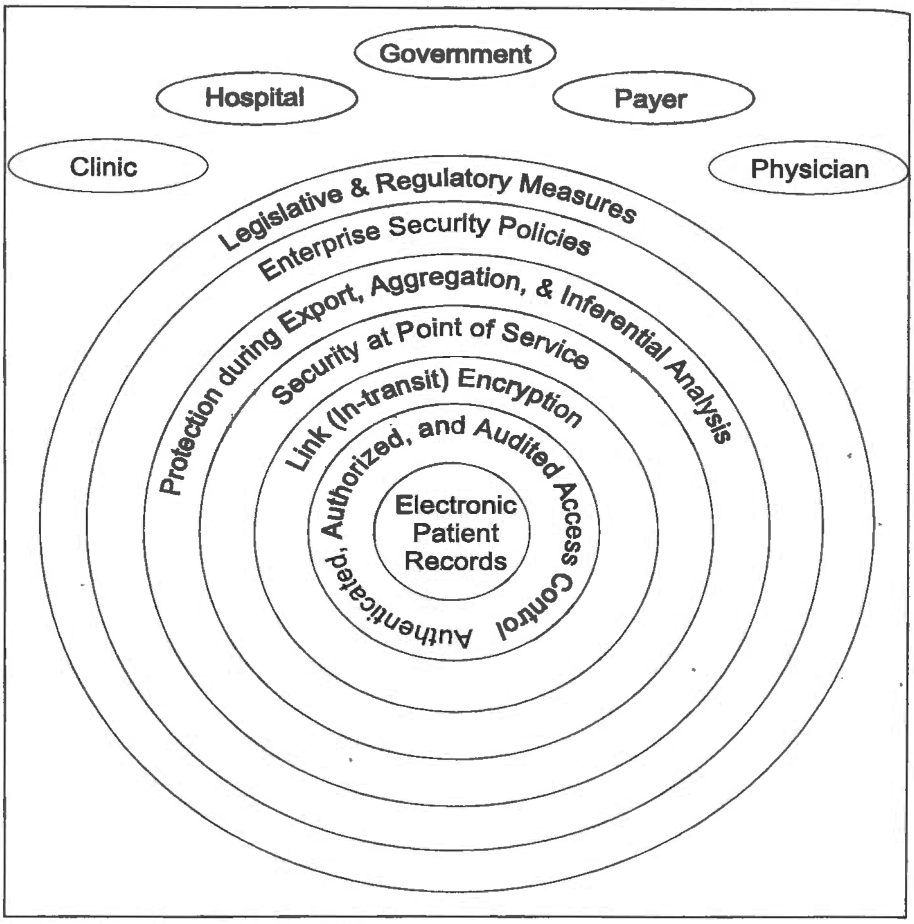

Figure 2. Layers of security measures.

1. Electronic health-care records can be protected by applications and servers that incorporate and abide by authenticated, authorized and audited access control facilities.
2. Link encryption can be employed to ensure the privacy and integrity of information while it is in transit over communication links.
3. Security at the point of service can include such measures as user authentication and screen locks to prevent improper access and accidental disclosure.
4. Protection measures, in accordance with enterprise and legislative measures can be employed to prevent the inadvertent export of information, reducing the risk of aggregation and inferential analysis. Emerging data exchange standards allowing selective record exchanges between health-care systems will also help address this issue.
5. Enterprise security policies consistent with emerging recommendations can help ensure that appropriate technical, administrative and procedural measures are employed to maintain the privacy of electronic health information.
6. Legislative and regulatory measures can provide broad guidelines that increase the protection provided for electronic health information and provide punitive measures for violations.

Collectively, these measures will ensure the confidentiality of electronic health information stored in the nation's health-care organizations and will enable the practice of telemedicine. Such forms of protection will enable individual measures to be reinforced or relaxed, depending on the capabilities of the others to provide the desired level of security.

In order to adequately secure health-care transactions, appropriate elements of the emerging computer-based security facilities must be utilized in the health-care organization's computing and network infrastructure, integrated into their servers and applications, and incorporated into their operating procedures. Such measures will provide true end-to-end security for collaborative telemedicine transactions. The development, demonstration and deployment of secure collaborative telemedicine applications, and the widespread dissemination of the results, will be crucial to encourage health-care providers to adopt these new solutions.

We believe that the incorporation of secure collaboration technology will have a profound effect on the health-care delivery system, engendering acceptance and confidence in users and becoming instrumental in fostering entirely new forms of health-care transactions beyond business transactions, such as Electronic Data Interchange (EDI) or the emerging electronic referral, to the formation of entirely new virtual health-care enterprises. As these technologies mature and their acceptance increases, we believe telemedicine will become commonplace, where an electronic house-call is just as routine as a visit to the local clinic.

Collaboration Technology for Health-care

Concurrent Engineering Research Center (CERC), an interdisciplinary research unit of West Virginia University, has been developing generic collaboration technologies using computers and communications networks since 1988. Developed under the sponsorship of the U.S. Department of Defense's Defense Advance Research Project Agency (DARPA), these technologies were originally envisioned to empower a geographically distributed tiger team to develop better quality products with less cost and less turn-around time. Computer-supported collaboration services [1] enable distributed participants to behave as though they were "virtually collocated". Basic services for enabling collaboration include support for information sharing, communication, coordination, corporate history management and integration. The generic technologies developed to facilitate concurrent engineering were adapted to the health-care domain and have demonstrated via the ARTEMIS project [2] that the current health-care framework can leap over the current state of the practice which involves the photocopier, the fax machine, phone lines and the proprietary hospital information system. This application of collaboration technology in the health-care telemedicine arena, funded jointly by DARPA and the US National Library of Medicine (NLM), was the first to enable health-care providers access to distributed clinical patient records utilizing the World Wide Web.

CERC's ARTEMIS system attracted the attention of the national media in the United States by illustrating the use of the World-Wide Web as a means to access electronic medical records. Developed in partnership with health-care practitioners, this system contained innovative solutions prior to their availability in commercial products for example, dynamic creation of HTML pages using medical record templates, CORBA/HTTP integration [3], Web browser customized to support coordinated multi-document electronic patient record browsing, support dictation of encounter notes, and Web-based document signoff facilities.

Meeting-on-the-Network (MONET) [4], a multimedia based desktop conferencing system with interoperability between workstations and PC platforms, developed at CERC, provides the basis for conferences between health-care providers. A Java-based white board supports multi-platform interoperable sharing of information during conferencing.

ARTEMIS and MONET, in combination, enable health-care providers to collaborate via video communications as well as access to medical information. They are currently undergoing field trials [5] and evaluations [6] at a set of rural health-care facilities.

Secure Collaborative Telemedicine

CERC is now engaged in a new three year contract under the sponsorship of the U.S. National Library of Medicine, to develop and deploy applications for secure collaborative telemedicine in rural areas of the United States and to evaluate its impact on the delivery of health-care. In partnership

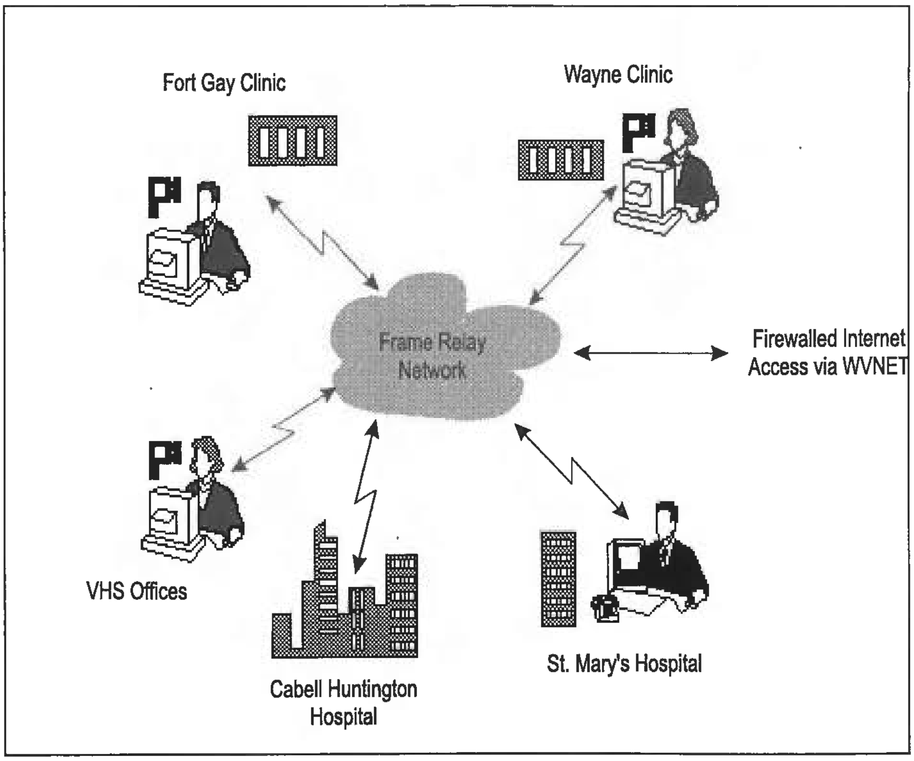

Figure 3. ARTEMIS communications infrastructure

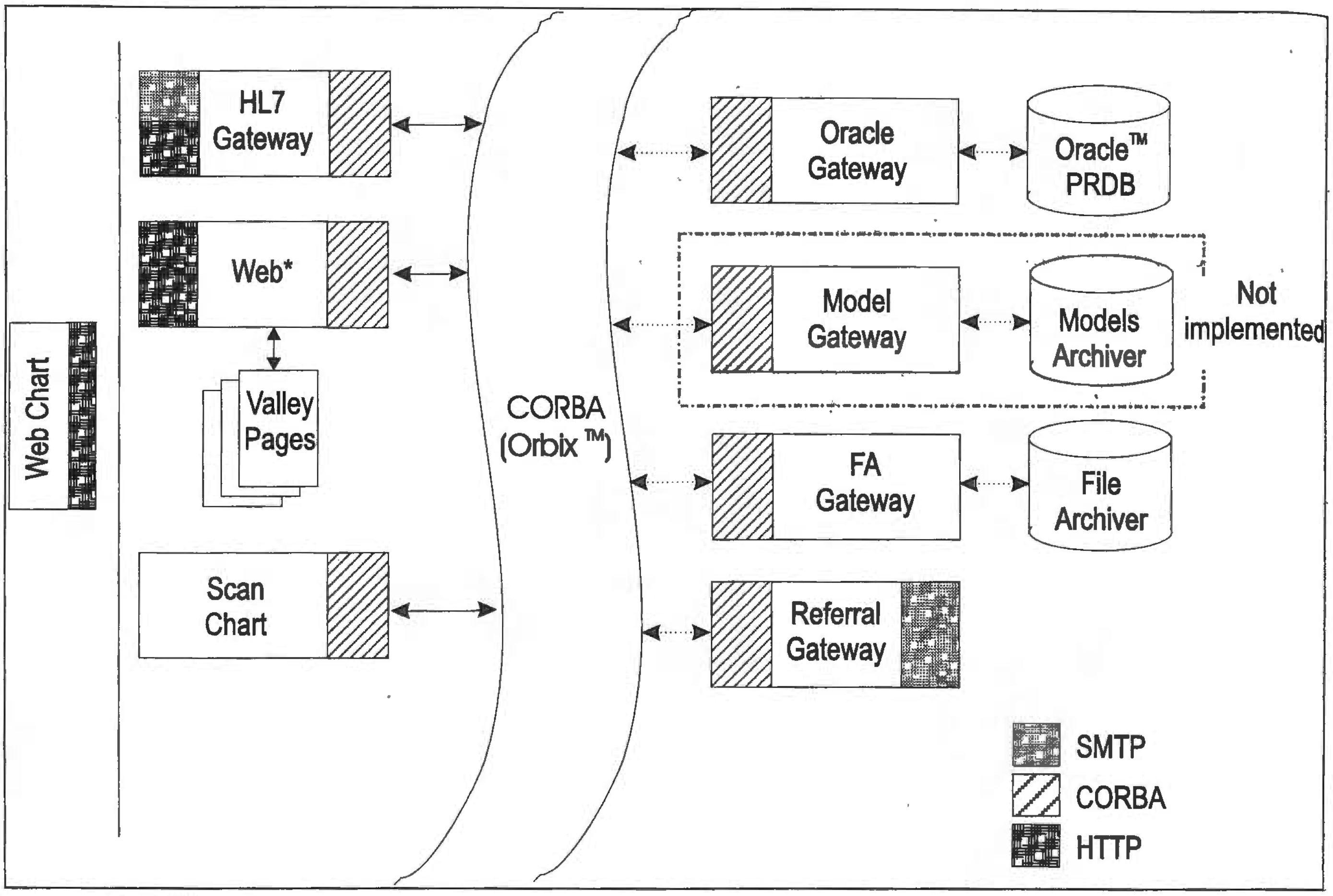

Figure 4. ARTEMIS architecture.

with health-care providers and health-care system vendors, CERC is developing telemedicine applications for deployment in three categories of health-care facilities to assess their impact on improving accessibility, reducing cost and improving quality of care, especially in rural areas such as the State of West Virginia.

We are developing a Secure Collaborative Telemedicine Architecture (SCTA) using the open systems approach and emphasizing the reuse of technologies already developed under previous projects or that are available commercially. We are designing a collaborative telemedicine system "software backplane" into which a variety of software modules could be "plugged," by embracing the object oriented approach and using the industry standard protocol known as CORBA (Common Object Request Broker Architecture) which is presently supported by over 600 vendors world-wide. It will employ bridge facilities to accommodate other standards, such as Microsoft's Distributed Component Object Model (DCOM).

A comprehensive secure collaborative telemedicine system should provide as its core capabilities:

- a security infrastructure that supports authentication and the secure transmission of private and confidential patient information
- transparent and easy access to distributed patient information
- a secure workflow in the context of patient treatment
- a secure consultation service in the context of patient information and patient treatment plan.

In our view, support for the above services constitutes the core backplane for telemedicine applications. Other services can be plugged into this backplane to provide a variety of custom support features to a variety of specific providers including:

- real-time or near real-time access to information gathered by instruments monitoring a patient;
- seamless access to clinical decision support systems and on-line knowledge repositories such as Medline.

The authentication services of the SCTA will support measures to restrict access to authenticated and authorized personnel.. We are adopting industry-standard cryptography solutions to develop a secure, open, collaborative technology infrastructure which supports the distributed components of our telemedicine applications. A number of promising solutions in this arena are being introduced, and we are evaluating these offerings, developing initial prototypes with commercial tools, for integration with our CORBA-based services.

We plan to employ Certification Authorities for managing public keys and PIN protected smart cards for storing private keys. Via a certification authority we will provide secure management and trustworthy disbursement of public keys and enable credential verification of health-care providers.

A smart card resembles a credit card in size and shape. However, a smart card stores information and instructions on an integrated microprocessor chip located on the card. There are two basic kinds of smart cards, a "memory" smart card and an "intelligent" smart card. The "memory" smart card's primary use is to store information, such as monetary value amounts which can be spent for various transactions, including pay phones, retail, or vending. The "intelligent" smart card contains a central processing unit (CPU) that can store and secure information. "Intelligent" smart cards offer read/write capability and thus information can be added and deleted as required by a particular application. Current smart card integrated circuit chips range in memory size from 1K to 8K bytes. In both instances, the information is stored in the integrated circuit chip and thus cannot easily be tampered with, unlike a magnetic stripe card which carries information on the outside of the card and can easily be copied. Smart cards are thus the primary means of storing the information necessary for encryption keys and electronic digital signatures. We expect PIN protected smart cards to be used in our telemedicine applications for the identification and authentication of providers, identification and authentication of patients, and storage of limited patient medical information.

We expect the SCTA services to be incorporated into our telemedicine applications which will be customized to meet the individual and organizational needs of the health-care facility. For secure operation it must work in concert with technological and administrative procedures in compliance with the security policies of the health-care network. External intrusion can be detected and curtailed through measures such as firewalls, dial-back modems, and strict monitoring of external incursions to the network. Internal misuse of private patient information can be deterred through the use of encryption, authentication measures, screen locks, audit trails and through enabling application-level security facilities. Periodic inspections of security policies and procedures will determine the efficacy of these measures and enable corrective action to be taken.

Telemedicine Applications for Rural Health-care

A set of three telemedicine scenarios have been identified that enable health-care providers to collaborate in the treatment of patients. These scenarios illustrate the utility of collaborative telemedicine technologies to improve the delivery of health-care at rural hospitals, clinics, and home-care sites:

1. Secure telemedicine for intensive care providers enabling remote access of Intensive Care Unit electronic patient data.
2. Secure telemedicine for mid-level providers (such as physician assistants and nurse practitioners) providing computer- aided diagnosis and collaboration with remote supervising physicians.
3. Secure telemedicine for home care patients through patient counseling information resources and support for near-time monitoring of patients with chronic ailments.

It is important to note that the above telemedicine applications could be realized with current technology. However, the challenges being addressed by this research effort are to enable these services while ensuring security of information, seamlessly integrating them into a health-care enterprise's overall support system, and ensuring their evolution with technology.

At this stage of the project we are primarily engaged in the requirements gathering and planning phase for these telemedicine applications. We are concentrating our technical efforts on the design of the SCTA which will provide the underpinning and essential services to be used in these applications. These applications define our vision for secure telemedicine in the targeted rural health-care facilities in West Virginia.

In the Intensive Care application, we plan to provide telemedicine support for an intensivist, a sub-specialist providing care for ICU patients, to remotely determine the condition of their patients, by reviewing their electronic ICU medical charts, examining data from bedside monitors, and conferring with ICU health-care providers on prognosis and interventions. At present, the ICU staff at the rural hospitals utilize the phone and the fax as means of conveying partial information to remote intensivists. Through the planned telemedicine system the intensivist could review current and detailed information and prescribe a course of action (medication, diagnostic tests, or preparation for surgical procedures). Timely access to information could provide a head start on procedures and improve the patient's chances of survival, or eliminate needless travel to the hospital. While commercial remote monitoring systems are available today, these solutions generally do not address transport security, relying on patient monitor networks that employ password-based access control. We are planning to utilize CORBA-based monitoring services leveraging the new IEEE 1073 Medical Information Bus standard in this application.

In the Mid-level Provider application, we plan to provide telemedicine support for mid-level providers such as Physician Assistants (PA) and Nurse Practitioners (NP). The PAs and NPs have substantial responsibility, yet they must be under the supervision of a physician. In rural areas, with small, yet dispersed populations it is necessary for the PAs, NPs and the supervising physician to cover separate clinics, affecting consultation and the amount of supervision. Yet, through the use of teleconferencing and electronic patient records, distance may no longer be a barrier. Computer-aided diagnosis and treatment support systems can further assist the mid-level providers in health-care delivery. Needless travel by patients can be eliminated and in such cases, the consultation may occur while the patient is still in the clinic. Furthermore, such a telemedicine application will allow physicians to increase their span of control by supervising more mid-level providers in outlying clinics thereby increasing the access to care and driving down the cost of health-care delivery.

In the home-care application, we plan to provide telemedicine support for home care patients and their health-care providers. Home-care patients having ready access to patient counseling information resources will be able to responsibly participate in the health-care delivery process and its outcome. By enabling patients with chronic ailments to provide information about their conditions this application will allow health-care providers to take timely intervention in the treatment of their patients. Health-care providers often spend time advising their patients about the treatment that they are advocating, identifying side effects of medications, and suggesting lifestyle changes that would improve their well-being. Home-care patients undergoing treatment for chronic ailments such as diabetes, hypertension, or obesity may benefit from computer-assisted counseling resources that provide quick access to detailed information. Rural home-care providers are even less equipped than their clinic-based counterparts to provide patient education brochures.

Home-care patients with chronic ailments, such as diabetes, will also benefit from closer interaction with their caregivers through computer-assisted reporting of their conditions which allow their health-care providers to monitor their progress closely without requiring frequent visits to health-care facilities. For instance, diabetic patients could provide periodic updates of their daily medical logs (blood sugar, weight, medication, well-being) and benefit from early intervention such as changes in drug dosage, diet, or be called in for further check-up. Morbidly obese patients may provide reports indicating their weight, deviations from prescribed diets, exercise, medication, and mental well-being. Through automated monitors and specially designed forms patients could provide periodic updates on their condition for review by their health-care providers. In the case of diabetes patients, such a system may allow the patient to be treated by a team of health-care providers (primary physician, podiatrist, nutritionist, or nurse).

Conclusions

We are confident that computer-supported collaboration technologies will enable health-care providers to improve the quality of care provided to their patients. Our own experience with ARTEMIS and those of other leading experiments such as TELEMED reinforce the belief that collaboration technology will help overcome barriers to quality health-care not just in small, scattered populations of rural areas, but reorient the very business practices of health-care. In the USA, legislative measures have been passed proscribing the potential disclosure and misuse of personal health information. Emerging technological solutions for cryptography hold out the promise for commercial transactions on the Internet. Collaborative health-care transactions will not be far behind.

References

1. Reddy YVR, Srinivas K, et al. Computer support for concurrent engineering. Computer 1993; 26:1 12-6.
2. Jagannathan V, Reddy R, et al. *An Overview of the CERC ARTEMIS Project*. CERC Technical Report Series. CERC-TR-95-002. Concurrent Engineering Research Center, West Virginia University, 1995:1-5.
3. Jagannathan, V, Almasi G. Integrating the WWW and CORBA-based environments. First Class 1996; 6:13-6.
4. Srinivas K, Reddy R, et al. *MONET: a Multi-media System for Conferencing and Application Sharing in Distributed Systems*. CERC Technical Report Series. CERC-TR-91-009. Concurrent Engineering Research Center, West Virginia University, 1991:1-18.
5. Reddy S, Shank R, Jagannathan V, Merkin B. A Virtual enterprise for rural health care through advanced communication and information technologies. In: *Annual Review of Communications*. International Engineering Consortium, 1996:631-6.
6. Galfalvy HC, Reddy S, et al. *Evaluation of a Community Care Network (CCN) System in a Rural Health-care Setting*. CERC Technical Report Series. CERC-TR-95-001, Concurrent Engineering Research Center, West Virginia University, 1995:1-5.

Address of the authors:
R. S. Raman, V. Jagannathan, K. Srinivas, S. Reddy, K.J. Cleetus, R. Reddy
Concurrent Engineering Research Center,
West Virginia University,
Morgantown WV 26506-6506,
USA.