1 Introduction

According to the 2003 National Healthcare Quality Report [2], the lack of timely and accurate data access is a major limiting factor in improving healthcare quality. Timely diagnosis and treatment require the collection, retrieval, and aggregation of various types of data from multiple sources, posing a major research challenge. Meanwhile, pervasive computing technologies, such as smart-cards, RFIDs (radio-frequency identification devices), sensors, and wireless computing platforms (Tablet PCs and PDAs) have emerged. These technologies enable pervasive data access anywhere, anytime, and on heterogeneous platforms, creating an excellent opportunity to make an immediate impact on the data access challenge in healthcare [24].

Pervasive technologies have the potential to empower both patients and medical personnel with more data control and accessibility, leading to improved healthcare quality metrics such as safety, effectiveness, efficiency, and human error rate [14]. More specifically, pervasive data access can contribute to the improvement in measurement, monitoring, diagnosis, emergency response, and treatment. For example, in medical emergencies, obtaining timely access to a patient's medical records allows the rescue team to provide faster, safer, and more effective treatment. In a hospital, using PDAs and Tablet PCs to collect and record patient data from different devices will save significant amount of time and prevent many human errors [12]. In a clinical environment, patients can use smart-cards and other smart devices to record symptoms before visiting the doctor, thereby improving the accuracy of symptom descriptions, especially intermittent symptoms. In summary, pervasive data access is expected to bring the following benefits: timely diagnosis and treatment, patient control of health data, reduction of errors (for example, medication errors [29]), and interoperability of data from different sources. Furthermore, pervasive data access plays a critical role in preparing and responding to national health emergencies, such as biological, chemical and nuclear terrorist attacks [24].

Although the adoption of pervasive technologies is a great opportunity with tremendous impact, there are new risks and challenges that need to be addressed before pervasive data access in healthcare can become a reality. Both the technology push and application (healthcare) pull call for research in critical aspects of pervasive data access, namely *integration, privacy, and usability*, under strict regulations [22]. Without addressing these challenges, pervasive data access may unwittingly compromise the healthcare quality instead of improving it. Furthermore, the adoption of pervasive technologies should not compromise the established patient - medical staff relationship.

Proposed Research The following directions will be pursued in which new research is essential to the adoption of pervasive data access in healthcare: (1) middleware support for integrated and context-aware data access; (2) methods to eliminate potential risks in privacy and security that are associated with pervasive data access; and (3) usability studies to improve user experience, user control of data [40], and society acceptance. More specifically, advances in science and technology will be achieved through the following research investigations:

- *Integrated middleware for pervasive data access* An underlying middleware system will be developed with an awareness of not only physical context, but also social and workflow context. The idea is to enable data access only in the *right* contexts, and to dynamically invoke data protection methods under potentially risky conditions. Therefore so that data mis-use and unwanted disclosure can be avoided. Data access management mechanisms will be investigated at two levels: the workflow level involves multiple data access sessions in the same workflow, while the session level involves multiple data access operations as well as data replicas in the same data access session. A middleware prototype will be implemented; and a number of healthcare applications will be developed on top of it.

- *Privacy and access control in pervasive environments* When integrating pervasive devices into healthcare, the security and privacy implications need to be investigated. New security protocols will be

developed to integrate pervasive devices (e.g., multi-purpose medical smart-cards) through the middleware; access control policies and mechanisms are expected to be fine-grained and context-aware; and user friendly interfaces will be designed and evaluated to give users more control over their privacy.

- *Usability of pervasive technologies* The use of pervasive technology in medical environments faces human task demands and time pressure. Furthermore, pervasive technology is intended to be used by people of various educational backgrounds and computer literacy, making it difficult to find the proper balance between usability and security. This balance will be investigated from the perspective of both patients and medical personnel, ensuring that privacy will be maintained at desired levels and that users of the system will be able to interact with it effectively.

- *Deployment and evaluation* The system prototype will be evaluated in terms of its impact on healthcare delivery. The success of the prototype will be evaluated via experiments conducted jointly with medical staff in Arnett Clinic and the Regenstrief Institute. The metrics of success will be defined by the research team, medical professionals, and hospital administrators. Feedbacks from the prototype deployment and evaluation will help in the adoption of pervasive data access in healthcare (Section 8 "Coordination Plan").

2 Motivating Healthcare Applications of Pervasive Data Access

The decentralized US healthcare system involves the following participants: patients, medical professionals (doctors, nurses), health insurance companies and pharmacies. Collaboration and exchange of information among these participants is required to provide high-quality care. However, access to information should be protected, and data release should be kept minimum just to allow healthcare delivery. In addition, legislation like HIPAA [22] adds to the complexity of the overall system. Some motivating healthcare applications of pervasive data access are as follows:

Smart-card as personal health history and current medication storage device Many countries are already using the smart-card (a credit card sized device that contains a computer chip and is capable of limited data storage and processing) as the healthcare identification card. Several experiments are also being run in the United States. Example systems include the University of Pittsburgh Medical Center and the Mississippi Baptist Health Systems [23]. In existing systems, smart-cards are used mainly for authentication. The card stores a small amount of information, for example: name, address, blood type, insurance information, and PIN (or fingerprint template). We propose to extend the use of smart-cards to store more medical information and to provide differentiated and fine-grained access control to the data stored in the card. Access may occur in different contexts, which require different security and privacy policies. Information that can be stored in the card include allergies, essential health history (that show genetic predisposition to certain diseases), and current medication. Some information will be under the control of the patient, some under the control of the doctor, and some under the control of the insurance company. Additional verification methods can be used when the smart-card is used for medical treatment. For example, the medical database can also include a picture. In the case of emergency, we envision the possibility of an emergency code that can be used to obtain the information.

Tracing the use of data-sensitive devices outside the hospital Devices like Tablet PCs and PDAs contain sensitive data (patient health information and treatment). We propose to track these devices by using RFIDs, and to apply adaptive protections (such as change of access privilege, anonymization, and encryption) to the data when the devices are used in risky environments.

Smart data Data downloaded on mobile devices can have embedded mechanisms that allow certain operations to be triggered automatically or to issue reminders to the human personnel asking for attention.

Examples include sounding an alarm when time constrained treatment must be performed and deleting sensitive data based on timeout or location change.

Automated patient treatment and compatibilities check When hospitalized, patients are typically given a paper bracelet used to track their identity and medication. We propose to use RFIDs as temporal identification. The benefits of this approach is that nurses can automatically verify the identity of the patient and of the prescribed treatment before applying it. An additional check for unwanted reactions among the different drugs can also be performed. This method has many implications on privacy. Several possible solutions include detecting un-authorized readers or employing a master-key to control the release of the identification number stored on the RFIDs.

On-line prescription renewal and order Regulations require patients to have prescriptions issued by doctors before going to pharmacies to pick up the medicines. Many conditions require long-term or permanent medication, while prescription is provided for a short-term such as one month. This requires the patient to either visit or call the doctor, whom in turn will inform the pharmacy that the prescription is renewed. An on-line prescription service is very useful for people living in remote rural areas, or for mobility challenged people. On-line communications between patients, doctors and pharmacies, together with the use of smart-cards as patient identification, makes the process of prescription renewal smoother, more accessible, and more accurate.

3 Integrated Middleware for Pervasive Data Access

3.1 Problem Statement

An underlying middleware system is needed to support applications involving pervasive data access. It will benefit application developers by avoiding the implementation of ad hoc and tedious mechanisms for data access management. The middleware architecture will be able to adapt to heterogeneous devices and dynamic network conditions in a pervasive environment, accommodating the differences in device interfaces, data processing, communication, and rendering capability in a systematic and customizable fashion [31, 39, 41]. Research in the following aspects of pervasive data access is critical to the successful deployment of the middleware system in real-world applications:

- *Session-level* integrated management: A data access session involves a series of operations on a data item, such as *read*, *write*, *migration*, and *replication*. To ensure proper usage and protection of data, there is a need for session-level mechanisms to enforce a valid sequence of data access operations, perform data protection functions (such as re-authentication, access privilege adjustment, and encryption), track data replica locations, and dispose data replica(s) upon session completion.

- *Workflow-level* integrated management: In healthcare applications, there are well-defined workflows involving the access to multiple data items. To ensure proper creation and execution of data access sessions in a workflow, integrated mechanisms are required to validate, monitor, and steer these sessions. These mechanisms are needed to prevent data mis-use and mis-disclosure because of an undefined data access session in the workflow.

Both session-level and workflow-level mechanisms are more challenging in a pervasive environment than in a traditional desktop environment. First, they require strong *context and situation awareness*: the same data access session may be valid in one context or situation, but invalid in another. Second, because of the device mobility and portability, data access control is more difficult to enforce: a user may be temporarily disconnected from the backbone network, and a device (such as smart-card or PDA) may be left unattended unintentionally, making it difficult to maintain the integrity and validity of data access sessions.

3.2 Related Work

Mobile and pervasive data access Pervasive computing realizes the idea of data and service access "anytime, anywhere, and using any device". GAIA [44] is a middleware system enabling the creation of active space in pervasive environments. Beyond traditional computing systems, it encompasses devices and physical spaces so that they can interact with each other as well as with users. In [13], a middleware system is presented that enables pervasive business processes and workflows. The Mobile People Architecture [37] provides a unified communication infrastructure for seamless messaging between people. In [41], application-aware adaptation for mobile data access is investigated, focusing on two characteristics: fidelity of data and agility of adaptation. The Puppeteer system [17] enables component-based adaptation of mobile applications, by leveraging the exported interfaces of applications as well as the structured nature of the data they manipulate.

Context awareness Context-awareness is one of the main focuses of pervasive computing. The Context Toolkit [18] provides conceptual framework and programming support for the acquisition and representation of context found in a rich space of context-aware applications. In [30], a system for context recognition at multiple levels of abstraction is presented. However, it does not address user intervention and social (rather than physical) context. A graph-based context aggregation and dissemination model is presented in [15], supporting the subscription to context information by multiple applications. In [6], the trade-off between system automation and user involvement has been identified. It is concluded that people are willing to give up partial control of applications for automatic context awareness, if the reward in usefulness is great enough. Our research will deepen the understanding of the system/user relation. Recently, context-aware security and privacy has received significant research attention [26]. A context-aware security service framework is proposed in [50] for formal and complex context modeling. In [25], a situation-based scheme is presented for the control over data publication and service provisioning. The goal is to achieve fine-grain user identity management under different contexts. However, it does not address the issue of context validation, as well as the relation between context and risk of data mis-use/mis-disclosure.

3.3 An Integrated Middleware System

We propose a middleware system that advances the existing technologies. The middleware provides APIs and mechanisms for pervasive and guarded data access. The novelty and challenges lie in the two-level (session and workflow) data access management for the prevention of data mis-use and unwanted disclosure, with strong context-awareness. Figure 1 shows the main components of the system.

- The *context engine* is responsible for the collection of raw context data, such as environment conditions from sensors and user/device locations from an RFID system. Based on the raw context data, the context engine will infer and validate the semantic-level context, which is defined in and applied to each workflow instance and data access session. The context engine may be implemented in either a centralized or distributed fashion, so that a global view of the current context can be maintained.

- An *access control manager* is associated with each data repository, which can range from a smart-card to a database. It enforces access control rules for data items in the repository. Furthermore, it may dynamically adjust the access control rules at the request of session managers (to be described next).

- A *data replica protector* is created for *each copy* of a data item. The data replica protector implements a number of self-protection methods for this replica, such as *encryption*, *anonymization*, *access privilege adjustment*, and *self-disposal*. These methods will be invoked by either the corresponding session manager, or by the protector itself when losing contact with the session manager.

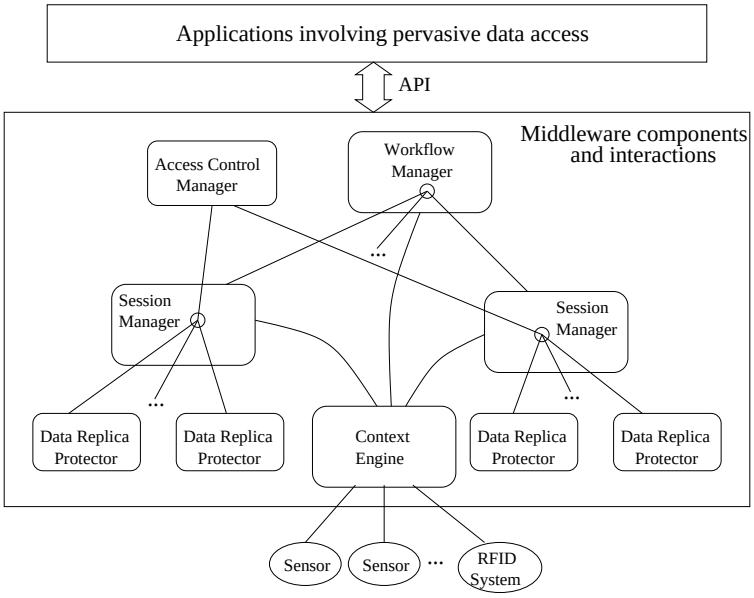

Figure 1: Components and interactions of the middleware system

- A *session manager* performs session-level data access management. During a data access session, it enforces valid data access operations and their sequence (for example, "*always start with user authentication and end with data replica disposal*"), adjusts data access control rules, invokes data protection methods, and tracks all replicas of the data item, all driven by change of context.

- A *Workflow manager* performs workflow-level data access management. During a workflow, it enforces the data access sessions defined in the workflow by validating the creation of a session, instantiating a session manager, and monitoring the status of each data access session. A workflow manager may oversee multiple session managers. With context-awareness, the workflow manager makes sure that no illegal data access session will be created.

3.4 Research Problems and Directions

Context inference and validation Context is modeled along multiple dimensions, such as time (when), location (where), presence of people (who), occurrence of events (what), and purpose of events (why). Under different contexts, the same user may be given different access privilege for the same data item. For example, a doctor uses a PDA to download a patient's record. When the doctor is in her office, she has full access privilege to the original record. When she goes to a meeting with other doctors, the original record will be replaced by an *anonymized* version. If she carries the PDA to a non-work area such as the cafeteria, the record downloaded to her PDA will be automatically encrypted or even deleted.

Contexts may not always be recognized and validated automatically, which is a problem faced by real-world applications. A uniform framework is also needed for the modeling, inference, and validation of context, especially along the subjective dimensions such as social and personal situations. This research will address the following problems:

- Context sensing devices may not be reliable and trustworthy at all times. The raw context data such as location, temperature, and human mobility need to be validated before they are used for semantic-level context inference. Such validation mechanisms will be developed in the middleware system.

- It is possible that in a context dimension, the corresponding sensing mechanism is not available. This is true especially in an outdoor or ad-hoc situation, where there is no full coverage by the communication and sensing infrastructure. In this circumstance, human users will have to identify and validate the context, at the *reminder* of the system.

- The *mapping* from raw context data (e.g., where, when, who) to semantic-level context (e.g., what, why, how) needs to be studied. The latter will be more meaningful to the steering and validation of application-specific workflows and data access sessions.

In the proposed middleware system, an intelligent and human-centered context engine for context sensing, inference, and validation will be investigated. A formal model for the specification of domain-specific context and for the mapping from raw context data to semantic context will be defined. Meanwhile, the context engine is expected to interact with human users for context validation and identification when they cannot be performed automatically. The challenge is to achieve a balance between context sensitivity and user convenience. A self-learning method will also be investigated so that the context engine can dynamically adjust its behavior such as reminder frequency for better usability (more details on usability study in Section 5).

Session-level data access management To avoid a mis-use or improper disclosure of a data item, integrated data access management is required for an entire session, rather than for individual data access operations. A data access session is expected to start with user authentication, and terminate with proper actions such as deleting the replicas of the data item. During the session, data protection methods should dynamically be invoked under different contexts that are associated with various risk levels. Furthermore, in a session involving data migration or replication, the replicas need to be kept track of. For a pervasive environment with strong privacy and protection requirement, the design of session manager faces the following new challenges:

- *Context-aware in-session data protection*: Different contexts involve different levels of risk of data mis-disclosure. The session manager must monitor the current context (from the context engine) and trigger data protection mechanisms when necessary. The mechanisms can be a change of access privilege by the access control manager, or a protection method execution by the data replica protector. For example, a highway emergency rescue operation has higher risk of undesirable data disclosure than an ER in a hospital. As another example, if a Tablet PC has been left unattended for some time, the risk of the data replica being accessed by unauthorized people will increase. After sensing these conditions from the context engine, the session manager will evaluate the situation and invoke appropriate protection methods.

- *Data replica tracking*: A data replica may be migrated from one machine to another device, or distributed to multiple devices. Within the same data access session, all replicas of the same data item need to be tracked and accounted for, because they should *only* be used during the current data access session.

- *Disposal of data replicas*: Another novel feature of the middleware system is safe and enforced data disposal. Without an enforced data disposal, it is possible that a properly authorized data access session leads to an unauthorized data disclosure. For example, a nurse connects a blood pressure monitor to a desktop PC, and the readings are then written to a central database. However, a replica of the readings is left in the desktop PC. Any person using the machine may now access the data replica without authentication. Therefore, safe data disposal should be enforced for each data replica generated during a data access session. A challenge is the *balance* between data access efficiency and data protection, especially for large-volume media data such as high-resolution images. Lazy

data replica disposal may be good for data access efficiency and thus for timeliness of diagnosis and treatment. However, it is more vulnerable to undesirable data disclosure.

Workflow-level data access management During a workflow execution, the workflow manager will validate the creation of every data access session, according to a workflow data access script specifying which data items can be accessed under what context(s). Any data access session not matching the specification should be denied. The workflow manager is expected to have a strong context awareness. In fact, the different steps or stages in a workflow can be modeled as social or business contexts *themselves*. The following problems will be investigated:

- *Workflow as context*: Before runtime, the specification of workflow stages defines the social or business contexts in which different data access sessions will take place. During runtime, the workflow manager will communicate with the context engine for runtime context information. Therefore, there is a need for an integrated framework for both workflow specification and context definition.
- *Validation and enforcement of data access sessions*: The workflow manager is expected to validate each data access session, in order to avoid unjustifiable data access in wrong physical and social contexts. Furthermore, the workflow manager should also enforce the *inter-session* constraints during a workflow - for example, "*the access session for data item X should not be started earlier than the session for data item Y*", or "*the sessions for X and Y should not take place in the same location*".

In summary, the following research tasks are proposed: (1) study the definition, inference, and validation of physical, semantic, and business (workflow) contexts; (2) study the session-level and workflow-level mechanisms for integrated data access management; and (3) prototype and evaluate the proposed middleware architecture.

4 Privacy and Access Control in Pervasive Data Access

4.1 Problem Statement

Because of the sensitive nature of medical data, adequate privacy protection is important. In a pervasive environment, medical data are accessed by devices with highly varying protection capabilities. First, this research will analyze the security and privacy implications of pervasive data access. Second, the challenge of limiting pervasive data access to authorized personnel will be addressed. One difficulty is that data may need to be accessed by previously unknown parties, such as paramedic personnel during an emergency. Another difficulty is that data access rules depend very much on the contexts in which the access occurs. Finally, this research seeks to empower users with more control over who can use their medical information. In other words, patients should be able to specify, within a limit, who is allowed to access their medical and other personal information in the system. The challenge is to design a user-friendly policy model and a user interface through which users can specify such policies.

4.2 Related Work

Attacks on pervasive technologies Technologies that provide pervasive data access include smart-cards, RFIDs, and other devices such as PDAs or laptops that communicate via wireless communication. All these devices are vulnerable to numerous kinds of attacks.

A number of attacks are possible on smart-cards. Through *Reverse Engineering* [5], the layout and function of the chip can be identified. *Power Analysis* techniques use the differences in power consumption

between manipulating a logic 1 and manipulating a logic 0 to learn secret information stored in a smart-card [38]. Finally, the card reader may emit electromagnetic signals hinting the data being processed. These signals could be intercepted by an attacker [43].

An RFID tag is a small and inexpensive microchip that emits an identifier in response to a query from a nearby reader. The significant advantage of RFID systems is the non-contact, non-line-of-sight nature of this technology. While having the potential to enable a host of pervasive applications, RFID systems are vulnerable to numerous privacy and security threats, as shown in [47, 54]. Several methods have been proposed to address privacy concerns for RFID. One method involves the design of a passive RFID device that can simulate many regular RFID tags simultaneously. The device, referred to as a "blocker tag" [28], can selectively "block" RFID readers and form a "privacy zone". Because RFIDs are limited in memory and cryptographic capabilities, some interesting non-cryptographic methods to address privacy issues have been proposed [27].

Many wireless devices use the Wired Equivalent Privacy (WEP) protocol, which is part of the 802.11 standard, to secure their communication. Designed to provide confidentiality, data integrity and authentication, WEP failed to achieve its security goals as shown in [11, 51].

Fine-grained access control Access control techniques, which govern whether one party can access resources and objects controlled by another party, are useful in protecting the confidentiality, integrity, and availability of information. Role-based access control (RBAC) [19, 20, 46] is an emerging approach to access control. In RBAC, permissions are associated with roles, and users are granted membership in appropriate roles, thereby acquiring the roles' permissions. In the context of an organization, roles are created for the various job functions and users are assigned and revoked role memberships based on their responsibilities and qualifications. Traditional access control schemes make authorization decisions based on the identity of the requester. However, in ad-hoc access control scenarios such as emergency care, the resource owner and the requester often are unknown to one another, making access control based on identity ineffective. Trust management [7, 8, 9, 10, 16, 32] is an approach to access control in decentralized distributed systems with access control decisions based on policy statements made by multiple principals.

Privacy control The W3C's Platform for Privacy Preferences Project (P3P) [53] is one of the major efforts to improve today's online privacy practices. P3P seeks to inform users about web sites' data-collection and data-use practices to enable users to decide whether to reveal personal data to the web sites. On the contrary, we seek to enable users to directly set the policies about who can access their data.

Security interface design principles Yee [56, 57] has developed an Actor-Ability Model that is used to describe the apparent conflict between the way that users expect their computers to operate and the ways that they can actually operate. The model is based on the capabilities available to the discrete actors resident on the user's computer. These actors might be the operating system or application programs. Ten principles are presented for user interaction design in secure systems that are applicable to current pervasive technologies.

4.3 Research Problems and Directions

Security vulnerability analysis In this research, we seek to understand the capabilities and limitations of smart-cards, RFIDs, wireless communication, and EPRs (electronic patient record systems), as well as the security and privacy implications of integrating them [36]. Some of these technologies are increasingly being adopted without a careful analysis. Research is needed before these technologies are widely used. In our analysis, we will investigate the following attack scenarios: capturing sensitive data, unauthorized manipulation of data, denial of service, the presence of impersonators and insiders, and attacks during exceptional situations such as emergencies.

Security protocols This research will develop secure communication protocols between pervasive devices and study the security and privacy implications of these protocols as well as those of the overall middleware

architecture. Issues that we plan to address are: designing protocols for multi-purpose smart-cards, designing efficient key management protocols for wireless devices [3, 4], providing protection of stored data and cryptography-based control mechanisms on data access operations.

As an example, the proposed security protocols will enable the following scenario: hospitals and clinics maintain medical information about patients in EPRs that allow online access. Hospitals or insurance companies issue smart-cards to patients as well as to physicians. A physician's smart-card is used mainly for authentication and access enabling. A patient's smart-card, protected by PIN or biometric information, stores the following information: (1) medical information about the patient - this information may be accessed by doctors, as well as by the patient at home; (2) information critical in medical emergency, such as demographics, blood type and allergies - certain information may be accessible by everyone, while the rest should only be accessible to healthcare providers; (3) pointers to online EPR systems where further medical information may be obtained; (4) authentication information that enables the patient to access her online medical record; (5) the patient's security/privacy preferences; and (6) healthcare management information such as insurance.

Each medical staff member has a portable device (such as Tablet PC or PDA) with a smart-card reader. This device is carried by the staff member. Each patient, when being treated, is given a portable device to store her current health information. This device also has a smart-card reader and is carried by the patient. The staff's device communicates with the patient's device. They may both communicate with an EPR through wireless communication.

Context-aware access control Access to medical information stored in a smart-card or in an EPR system needs to be restricted to legitimate parties. In healthcare, data may need to be accessed by previously unknown parties. However, it is impossible to enumerate all medical staff members in a policy. And the traditional approach based on identities and access control lists (ACLs) does not provide an effective solution. We propose to investigate the *trust management* (TM) approach, in which policy statements issued by multiple authorities are combined to make authorization decisions. These statements can be carried in cryptographically signed credentials that resemble letters of recommendation through which issuers attest to precise and limited trust relationships with credential subjects. For example, a healthcare staff member may carry a credential issued by her hospital. The hospital has a credential issued by the healthcare authority. Thus, through a *chain of credentials*, a previously unknown healthcare staff member may be authenticated and given access to a patient's medical information.

In healthcare, data access conditions depend very much on the contexts in which the access takes place. In a life-threatening context, most rules can be broken in order to save lives. On the other hand, one should minimize the risk of attackers exploiting this relaxation to break rules for malicious purposes. To illustrate different levels of access allowed in different contexts, the following scenarios will be examined:

- The patient accesses the smart-card and the EPR system from a private and trusted computing device (a home PC). In this case, the smart-card has to be activated (e.g., using PIN) in order for any access to occur. Otherwise, anyone who obtains the smart-card can access the information. In this scenario, the patient should be given *read* access to most information stored in the card and in the EPR system. The patient should also have the ability to configure security/privacy policies to a certain extent. However, the patient should be restricted from modifying the medical data, indicating that the patient does not have a total control over the card.

- A medical staff member accesses the record of a patient in the EPR system without the patient being present.

- The patient is being treated in the home hospital, which issues the smart-card and maintains the EPR system. The patient is using the mobile device provided by the hospital. Three situations may arise:

(1) The patient is accessing the information herself without the presence of medical staff. The patient may wish to restrict her access to the card, since she may not fully trust the device, which could be a Trojan horse planted by attackers. (2) Both the patient and the doctor are present with their own smart-cards. Both cards are activated. In this case, both reading and writing of medical information in the card may be allowed. (3) In an emergency, the smart-card is with the patient. However, the patient is unable to activate the card. In this case, the inactivated smart-card may be combined with the doctor's smart-card and possibly with other evidences to gain emergency access to the patient's medical record.

- The patient is being treated in a hospital or clinic that is not her home clinic. Again, all three scenarios considered above are possible. However, data accesses should be even more limited because of the reduced trust in the 'out-of-home' environment.

This research will lead to methods that will allow access in different contexts, such as emergencies and mobile clinics, without compromising the security goals. In prior work, we have developed a family of Role-based Trust-management languages, called RT [33, 34, 35]. RT combines the strengths of RBAC and TM systems. Using RT, one can specify access control rules based on the authenticated attributes of the requester, such as certified physicians as well as the current context. Building on our prior work, a context-aware, fine-grained, and dependable access control manager (Section 3) will be developed as part of the middleware system to mediate access to medical data. The access control manager is driven by context-aware session managers as well as by the access control requirements of different stake holders, such as physicians, patients, hospitals, and insurance companies.

Usable interface for privacy This research will lead to a user interaction model and a user interface to enable users to control and/or audit the access to their medical information. We envision a framework that is easy to use without requiring the user to be a security expert. Yee's principles for designing security interfaces [56, 57] will be evaluated and enhanced. Some of the principles are (1) *Path of least resistance*: the most natural way to do any task should also be the most secure way; (2) *Explicit authorization*: a user's authorities must only be provided to other actors as a result of an explicit user action that is understood to imply granting; (3) *Visibility*: the interface should allow the user to easily review any active actors and authority relationships that would affect security-relevant decisions; and (4) *Expressiveness*: the interface should provide enough expressive power to describe a safe security policy without undue difficulty, and to allow users to express security policies in terms that fit their goals.

In summary, the following research tasks are proposed: (1) analyze the security and privacy implications of integrating pervasive devices into healthcare environments; (2) develop and analyze security protocols to integrate these devices through the middleware; (3) develop an access control manager in the middleware system that provides fine-grained and context-based access control; and (4) develop and evaluate a user friendly interface to empower users with more control over their privacy.

5 Usability of Pervasive Technologies

5.1 Problem Statement

A major requirement for pervasive technologies when used in healthcare is to protect patient privacy and to comply with current legislation [22]. Many security features rely on individuals to implement and use them, and they will not accomplish their intended objectives if users do not implement the security measures properly. This places a burden on administrators to select security methods that will ensure maximum protection while promoting the acceptance and compliance of users. Furthermore, if users perceive that the

information stored on using a particular pervasive device is not protected or that its features are difficult to use, they may respond with extreme resistance to adopting the technology.

Usability is a means to help ensure both that the information can be accessed by appropriate parties when needed and that security can be maintained. Usability encompasses (1) the ease with which a device can be used; (2) the ease with which people can learn how to operate a device; (3) the efficiency of the device; and (4) the preferences users have regarding the device design [58]. It is widely acknowledged that "human interaction is the Achilles heel of information security" [48]. Since the security of a system is only as strong as its weakest link, improving the usability of the technology will, by default, increase security. Usability is an important and challenging task in this research because the intended users of this technology are people in the general public, many of whom are not technically savvy.

This research will investigate how to provide high usability in pervasive medical environments, by focusing on two aspects. (1) Design with usability concern: while designing the pervasive system for medical data access, the usability is a primary consideration; (2) Iterative usability evaluation to improve usability: we plan to perform usability study of our design and implementation throughout the duration of this research and use the results of such studies to improve the system. Increasing usability will not only increase the efficiency of the system, but it will also promote the ease with which the users interact with the device.

5.2 Related Work

Usability and pervasive technologies The use of reusable passwords provides an illustration of the need to find a balance between security requirements and usability requirements for a security method to be successful. Users tend to write passwords down, or select easy-to-remember passwords that can be easily broken, thus compromising the security of the system. The security can be enhanced by placing various constraints on the password selection, at the expense of making the method more difficult for users.

Schultz et al. [49] performed an appraisal of usability issues in information security methods that included not only password-based authentication, but also other authentication methods such as biometrics, smart cards, and token devices. They also provided a taxonomy of usability issues associated with maintaining data integrity, confidentiality, and availability, and with detecting intrusions. Schultz et al. noted that there are significant usability issues associated with all methods of security and emphasized that security methods need not only to be designed to be usable but also must be accepted by users. Whitten and Tygar [55] identified five properties that make security inherently difficult for user interface design: (1) the unmotivated user property: security is (at best) a secondary goal of users; (2) the abstraction property: security policies are usually phrased as abstract rules that are incomprehensible to users; (3) the lack of feedback property: it is difficult to provide good feedback for security management and configuration; (4) the barn door property: once a secret gets out, it is out; information disclosure cannot be reversed, thus errors are often fatal; and (5) the weakest link property: the security of a system is only as strong as the weakest link.

Trust and usability Research on consumer behavior shows that users tend to trust devices that are highly usable more than those that are not [52], which can result in higher acceptance of, and preference for, the device. Because security is necessary to protect patients' private information, it is important that pervasive technologies be designed to be appealing to the user, both in terms of ease of use and ease of learning. If users perceive a device to be unusable, they may totally reject the technology, or worse, engage in nonsecure behaviors.

Usability principles Saltzer and Schroeder [45] identified eight design principles for building secure computing systems which have become standards of the computer security lexicon. The eighth principle is psychological acceptability, about which they wrote "It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly." Although almost 30 years have passed since this statement was made, knowledge on how to design devices that are

both usable and secure is still limited. It was not until recently that the security, human factors, and HCI communities turned their attention to the usability of security technologies.

Usability modeling and evaluation methodologies Usability is not a single, one-dimensional property of a user interface. According to Nielsen [40], usability has multiple components, being associated with the following five usability attributes: learnability, efficiency, memorability, minimal errors and satisfaction. There are two common approaches to usability evaluation [58]: inspection-based and user-based methods.

Inspection-based methods are usability evaluations performed by usability experts and can be classified in heuristic analysis and cognitive walkthrough. The first consists of having the expert evaluating the system and interface to see if it adheres to accepted usability guidelines, standards, and best practices. In the second, the expert uses the device to perform specific tasks from the viewpoint of the end user and notes aspects of the system or interface that can create difficulty for users. Inspection methods can be applied early and throughout the design process. They can be used efficiently to identify the characteristics that influence the system's performance.

Empirical user testing are methods where evaluation of the device is done by examining or observing representative users as they perform specific tasks with the device. With usability lab evaluations, users are encouraged to think aloud while performing the tasks. Thus, the method not only reveals usability problems, but also provides data concerning the user's thought processes as they perform the task and their preference regarding the device design.

5.3 Research Problems and Directions

Enhancing usability by design This research will investigate how to improve the usability for pervasive technologies in the following aspects:

- Evaluate the ease with which users can specify their privacy preferences and communicate their preferences to medical information systems. Users may not be able to articulate their privacy concerns, but we can evaluate their behaviors to identify them. For example, a user might verbally indicate that she would allow an insurance company to access her medical history. However, if given different scenarios of a patient and her medical data and asked whether the patient in the scenario should provide each piece of information to the insurance company's representative, the user may show that she does not want to reveal certain types of information to insurance companies.

- Determine the best privacy specification mechanisms by comparing, evaluating, and selecting the best expression mechanisms (e.g., languages, interfaces) of existing privacy preference tools and then optimizing these mechanisms for the medical environments. Research on human performance shows that people process information and respond differently under low stress and high stress conditions [42]. We will evaluate how people interpret different expressions of privacy specification under different stress levels and how to best organize and present information to both doctors and patients.

- Examine methods to effectively allow patients to select and specify different levels of privacy. We will evaluate the effectiveness of different interface designs at allowing patients to specify or modify their privacy preferences. We will also be concerned with implementation of both "canned" privacy choices and custom-made choices.

- Ascertain the proper balance between usability factors and security so that privacy can be maintained and feedback can be provided to users (e.g., to alert users to potential loss of privacy). We will determine what level of security precaution can be enforced that is acceptable to the end users and evaluate the effectiveness of different methods for alerting users when there is potential of intrusion.

- Implement optimal privacy enforcement mechanisms for both normal operations and emergency situations in medical environments. For example, a smart card can be programmed with four security levels: "read only," "add only," "update only," or "no access." Access of the medical information can also be designated so information can be accessed by the cardholder only, a patient-authorized third party (e.g., the patients family doctor), or a non-authorized third party. One question that arises is when is it appropriate to "override" a privacy setting in the event of an emergency where an unauthorized doctor in the emergency room needs to know the patient's medical history? Should an "ask for forgiveness, not for permission" rule be allowed in these emergency situations? If so, we will evaluate the best way to implement such circumvention policy and track its usage.

Iterative usability evaluation We plan to measure and enhance the usability of the proposed system using a variety of inspection-based and user-based methods. In the early design phases, we will primarily rely on inspection-based methods; however, we will use focus groups and other user-based techniques to ensure that the design matches well with the target users' mental models and expectations. Once the system has been developed, extensive formal user testing will be performed with different groups of users: system administrators, doctors, nurses, emergency medical personnel, and the different categories of patients (e.g., elderly, handicapped, adults, children, and patients on medication).

The proposed research will investigate the ability of system administrators to specify the privacy policies for the system; patients to specify and check their security preferences, as well as audit the record of access to their information; and hospital personnel being able to access particular pieces of medical information in different "emergency" and "non-emergency" settings. Due to the critical nature of the "emergency" settings, early usability evaluations of the system will simulate the physical and cognitive demands present in emergency situations (time-pressure, stress, and fatigue).

Sample experiment We plan to conduct a series of experimental studies to evaluate the usability of privacy specification language and context-aware interfaces. A sample experiment is briefly described as follows:
Purpose: Evaluate the ease with which system administrators and novice users can set privacy levels and the ease with which users can review their privacy settings and audit the use log with several different interface displays.
Input parameters: Display mode (e.g., text vs. graphic), display device (e.g., laptop, PDA, desktop computer), organization and layout of displayed information, and presentation and organization of system features.
Output parameters: Performance time, success rate, and types of errors (omission error: forgetting a step in the process; commission errors: performing the wrong action, performing the correct action at the wrong time) will be evaluated.
Method:

- Part A: Setting privacy levels. Two groups of participants, current system administrators (experts) that would be implementing the system and students from Purdue University (novices), will be given basic training with the proposed system so that they are familiar with the system's functionality. Each group will then receive a series of "fake" patient files for which the patients have specified the level of security that they desire. Each group will be asked to input the data into the system using different devices, display modes, and presentation/organization of information.

- Part B: Checking privacy preferences and auditing privacy information. Three groups of users (elderly, middle-age, young adults) will be asked to use the proposed system to check the privacy settings and audit logs for a series of "fake" accounts.

Analysis:

- Setting privacy levels: Separate analyses of variance will be performed on setup times, successful completions, and error rates, as a function of user group, different devices, display modes, and presentation/organization of information. A content analysis of error types will also be performed.
- Checking privacy preferences and audit logs: Separate analyses of variance will be performed on verification times, successful verification rates, and error rates, as a function of user group and task (checking preferences vs. checking an audit log). A content analysis of error types will also be performed.

6 Education and Outreach Activities

Goals and objectives The goals of education and outreach activities are to: (1) enhance the research and education capacity of faculty, graduate students, and undergraduate students; (2) integrate pervasive computing, middleware, usability, and privacy research into mainstream courses in computer science as well as in other disciplines such as nursing and psychology; (3) enhance the awareness and acceptance of pervasive technologies through training and education for both the general public and healthcare professionals.

The specific approaches for accomplishing these goals include: (1) increase the skills in privacy, usability, and middleware of participating faculty so that they are better prepared to teach and conduct research in their home departments; (2) increase the curriculum offerings in the areas of computer science, nursing, and psychology; (3) increase the number of students from healthcare disciplines who participate in pervasive computing and privacy education/research programs; (4) increase the number of capable professionals who can advance the integration of emerging technologies into hospitals and clinics.

Strength and challenge in minority education Minority programs have been established at Purdue in CERIAS and in other schools at Purdue. These programs are created at *multiple* levels to address *different* key transition points of students. The Graduate School offers the Historically Black Institution (HBI) Visitation Program at Purdue. The education and outreach activities will have a focus on privacy and emerging pervasive technologies. The challenge is the lack of teachers with multi-disciplinary backgrounds in healthcare, privacy, and pervasive computing.

Partners for knowledge transfer and diversity The education and outreach activities involve partners both inside and outside Purdue University. **Inside Purdue**, we are supported by the Office of Vice President for Human Relation, as well as minority programs of CERIAS, Schools of Nursing, Science, Engineering, Technology, Management, as well as the Horizons Learning Community. **Outside Purdue**, our partner medical institutions (Arnett Clinic and Hospital, Regenstrief Healthcare Center in IU Medical School) have also made strong commitment to knowledge transfer and education. A prototype in a *living laboratory* environment will be developed in Arnett Clinic and Hospital. The living laboratory model will be made *reproducible* for adoption by other medical institutions. All software systems, performance/usability analysis tools, and documentations will be publicly available.

Knowledge transfer formats and media To make knowledge transfer more effective and pervasive, we plan to generate knowledge transfer materials at multiple levels, for each technical topic in privacy, usability, and middleware. These knowledge levels range from background and awareness education targeting the general public, to hands-on demos and tutorials for patients, nurses, doctors, and other healthcare professionals, and to advanced research-oriented publications and system prototypes for researchers, faculty, and graduate students. In these materials, we will address the need of people with disabilities and methods to enhance security and trust in their interactions with pervasive information systems, such as alternative interfaces and additional integrity check mechanisms.

We will set up a web portal to disseminate knowledge about privacy and pervasive technologies. Such portals can be easily customized to fit the education background and interests of different users. On-line

interest groups will be created so that students can join groups of their interests and participate in discussions. Such interest groups are especially helpful in bringing together healthcare professionals from different parts of the country for the sharing of experience and support.

7 Results from Prior NSF Support

Prior NSF support for Professor Bhargava: Experiments in Adaptable Distributed Systems (CCR-9901712, 08/99 - 07/02) and Secure Mobile Systems (CCR-0001788, 09/00 - 09/03).

Shalab Goel and Ahsan Habib have got their Ph.D degrees. Eight undergraduate minority students and women worked as research assistants on a variety of experiments and participated in research. Two minority women graduate students participated. A few selected publications are listed:

1. E. Pitoura and B. Bhargava, "Data Consistency in Intermittently Connected Distributed Systems," *IEEE Transactions on Knowledge and Data Engineering*, Vol. 11, No. 6, pp. 896-915, Dec. 1999.
2. A. Zhang, M. Nodine, and B. Bhargava, "On Semi-Atomicity for Flexible Transactions in Distributed Database Systems," *IEEE Transactions on Knowledge and Database Engineering*, Vol. 13, No. 3, pp. 426-439, 2000.
3. B. Bhargava and M. Annamalia, "A Framework for Communication Software and Measurements for Digital Libraries," in *International Journal of Multimedia Systems*, Vol. 10, pp. 205-235, Jan. 2000.
4. B. Bhargava, "Secure Mobile Systems," in Proc. of *International Conference on Mobility in Databases and Distributed Systems*, London, United Kingdom, pp. 1-7, Sep. 2000.
5. B. Bhargava and Y. Zhong, "Authorization Based on Evidence and Trust," in Proc. of *International Conference on Data Warehousing and Knowledge Discovery (DaWaK)*, Aix-en-Provence, France, Sep. 2002.
6. A. Habib, M. Hefeeda, and B. Bhargava, "Detecting Service Violations and DoS Attacks," in Proc. of *10th Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, Feb. 2003.
7. Y. Lu, W. Wang, Y. Zhong, and B. Bhargava, "Study of Distance Vector Routing Protocols for Mobile Ad Hoc Networks," in Proc. of *IEEE International Conference on Pervasive Computing and Communications (PerCom)*, Dallas Fort Worth, Texas, Mar. 2003.
8. W. Wang, Y. Lu, and B. Bhargava, "On Security Study of Two Distance Vector Routing Protocols for Mobile Ad Hoc Networks," in Proc. of *IEEE International Conference on Pervasive Computing and Communications (PerCom)*, Dallas Fort Worth, Texas, Mar. 2003.
9. B. Bhargava, Y. Zhong, and Y. Lu, "Fraud Formalization and Detection," in Proc. of *International Conference on Data Warehousing and Knowledge Discovery (DaWaK)*, Prague, Czech Republic, Sep. 2003.
10. M. Hefeeda, A. Habib, B. Botev, D. Xu, and B. Bhargava, "PROMISE: Peer-to-Peer Media Streaming Using CollectCast," in Proc. of *ACM Multimedia 2003*, Berkeley, CA, Nov. 2003.
11. B. Bhargava, X. Wu, Y. Lu, and W. Wang, "Integrating Heterogeneous Wireless Technologies: A Cellular Aided Mobile Ad hoc Network (CAMA)," accepted for publication in *ACM Special Issues of the Journal on Special Topics in Mobile Networking and Applications (MONET)*.

NSF research grants allowed Professor Bhargava to develop and enhance courses at both undergraduate and graduate level with experimental studies. This has resulted in his induction in the *Purdue's Book of Great Teachers*.

8 Coordination Plan

Expertise of the research team The research team includes researchers from different departments in Purdue University. It will integrate their expertise in Computer Science, Nursing, and Psychology. Dr. Robert Hannemann, a physician with thirty years of pediatric practice, has appointment in Biomedical Engineering. He has experience in introducing new technologies into healthcare; and he will be instrumental in building the channels between healthcare professionals and the research team. The usability studies will be conducted in cooperation with Professor Robert Proctor and Dr. Kim Vu in the Psychology Department. The research team has been working closely with Dr. Michael Skehan, physician and Chief Medical Officer of Arnett Health Systems. The Regenstrief Foundation for healthcare based in Indianapolis is in the process of establishing a long term relationship with Purdue. This will lead to experiments in the application of high technology to healthcare, in the form of prototyping at Purdue followed by empirical studies in the hospital of Arnett Clinic, Lafayette and in Regenstrief Health Center (as part of Indiana University Medical School), Indianapolis. Affiliated with CERIAS (Center for Education and Research in Information Assurance and Security) and CWSA (Center for Wireless Systems and Applications) at Purdue, the team is in an excellent position to investigate pervasive data access and its privacy and security implication.

The unique expertise of each team member is described as follows:

Dr. Bharat Bhargava (Co-PI)'s research involves both theoretical and experimental studies in distributed systems. In particular, he is conducting research in pervasive computing and have published in the area of mobile systems, ad hoc networks, and distributed systems. Dr. Bhargava has implemented a large medical information systems at Wishard Hospital in Indianapolis and collaborating closely with Regenstrief Health Center. He is also involved in designing the networks and communication system for the Arnett Hospital that is being set up in Lafayette. He will teach a course in Pervasive Systems in Fall 2004 and has graduated the largest number of Ph.D students in the Department of Computer Science at Purdue (including five women).

Dr. Karen Chang (Co-PI) has practiced as a registered nurse since 1973. She is an expert in applying information technology to the improvement of patient care delivery and nursing education. She has received four interdisciplinary grants since 2002. She is currently working with computing technology professors in developing an electronic nurse's worksheet loaded in Pocket PCs and Tablet PCs. This electronic worksheet interfaces with mainframe to retrieve patient data and is designed to reduce the time that nurses spend in shift report. Her other project is related to the development and evaluation of a Diabetic electronic Management system using wireless Pocket PCs with access to Internet database.

Dr. Robert Hannemann (Senior Personnel) is a physician who has worked in the largest clinic (Arnett) in Lafayette as a Pediatrician. He is involved in the development of the new Arnett hospital in Lafayette and is working at Purdue in the Biomedical Engineering Department. He is involved in the proposal that will set up the Regenstrief Institute for Healthcare at Purdue. He has investigated error and privacy issues and the use of various high-tech devices in improving healthcare.

Dr. Ninghui Li (Co-PI) is an expert in information security, with expertise in access control, trust management, trust negotiation, policy languages, and cryptography. He has done extensive work in access control in open, distributed systems. Recently, he studied the usability aspect of security and privacy. Dr. Li and Dr. Nita-Rotaru have been collaborating on access control and group communication systems in CERIAS.

Dr. Leszek Lilien (Senior Personnel) is an expert in identifying vulnerabilities and threats in database systems and networks. He has identified a variety of scenarios under which privacy can be compromised in medical information system work flow and in the use of pervasive technology.

Dr. Cristina Nita-Rotaru (Co-PI)'s expertise is in designing survivable distributed systems deployed over wired and/or wireless networks. She is the architect of Secure Spread, a system providing secure group communication services and employing the first robust key agreement protocol. Secure Spread was selected

as one of 12 technologies that appeared on a DARPA DVD summarizing the accomplishment of 6 programs and it was selected to participate in JWID 2004, a large coalition experiment. She teaches Cryptography and Security/Privacy Topics in Networking and Distributed Systems, and co-teaches an interdisciplinary course entitled *Wireless Revolution*.

Dr. Robert Proctor (Senior Personnel) has published over 130 articles relating to the areas of human performance and human factors. He is a fellow of the American Psychological Association and American Psychological Society, and an honorary fellow of the Human Factors and Ergonomics Society. He has authored and edited several books on human factors and human-computer interaction. Recently, he has been conducting research on human factors issues in information security.

Dr. Kim Vu (Senior Personnel) is co-editor of the Handbook of Human Factors and Web Design (in press). She has expertise in the areas of human performance, human factors, and human-computer interaction, and has over 30 publications in these areas. She is a member of the Human Interface and the Management of Information Board for the 11th International Conference on Human-Computer Interaction. She has co-taught a tutorial on human factors issues in information security and is currently conducting research in this area.

Dr. Dongyan Xu (PI) is an expert in pervasive middleware systems. He has conducted research in QoS-aware middleware to support distributed services and applications in ubiquitous and pervasive environments. His Ph.D. work was part of the GAIA middleware system for smart space environments developed at UIUC, with a focus on QoS and context aware adaptation for pervasive multimedia applications. More recently, his research group is developing a middleware architecture for collaborative data streaming, protection, and provenance.

Collaborative research The research team brings together expertise in distributed systems and middleware architectures (Bhargava, Xu, and Nita-Rotaru), wireless and pervasive computing (Bhargava and Xu), privacy (Nita-Rotaru, Li, Lilien, and Xu), usability design, evaluation, and experiments (Li, Proctor, and Vu), and healthcare (Bhargava, Chang, and Hannemann). Bhargava, Xu and Nita-Rotaru have been involved in building, deploying, and evaluating large systems.

Weekly seminars/meetings will be held to discuss progress as well as research results. Task-oriented teams of graduate and undergraduate students and faculty will be formed to deal with specific research problems and experiments. The team will be based in a laboratory called RAID in the Computer Science Building. All experimental facilities, benchmarks, and tools are available for use by faculty and graduate students.

A middleware system called Promise [21] is available for further extension in this research. A system prototype called TERA (Trust-enhanced role assignment) [1] has been implemented and widely used to establish levels of trust and privacy. Bhargava and Xu are advising Ph.D. students in middleware systems. Bhargava and Li are working on models of trust with a Ph.D student.

Nita-Rotaru and Li are working on privacy issues and access control in group communications. Bhargava, Hannemann, and Xu are working with Regenstrief Health Center and Arnett Clinic in integrating pervasive and wireless technologies with clinic and hospital operations. Chang has been developing an electronic worksheet for nurses in Pocket PCs and Tablet PCs. Bhargava and Xu have working relationship with Cisco, IBM, Motorola, and Microsoft for research in pervasive communication and immersive collaboration middleware for distant education and training. Li and Proctor are working with Vu on building human-computer interfaces for a variety of applications and are in the process of conducting experiments.

The team members are offering research seminars to Ph.D. students in the area of privacy, trust, network security, pervasive applications. This creates a rich source of Ph.D. students for conducting the proposed research. A course on wireless revolutions has been offered to undergraduate students. A number of minority undergraduate students are involved with team members and will benefit from experiencing this exciting application. The team is working on identifying challenges in educating healthcare professionals in adopting

pervasive technologies. The members are working with medical professionals in staff training to prepare for prototype deployment in clinics and hospitals. Especially, Lilien, Xu, and Bhargava are working on tutorials for the promotion of user awareness of system vulnerabilities and threats.

Deployment and evaluation Advances in technology in the past decade have brought significant benefit to common users. The time-tested medical practices only change in small steps. This research is an attempt to bring realistic success to the improvement of healthcare quality. In collaboration with our partner medical institutions, the proposed prototype will be deployed in real medical facilities and be evaluated by medical professionals. We will work with doctors and nurses in Arnett Hospital and the Regenstrief Institute, who will identify benefits as well as problems of the prototype based on their professional experience and standard criteria. Several team members have worked in hospitals themselves, and have experience in applying computer science to make medical information system secure and reliable. They have been involved in measuring improvements in patient-doctor interaction and timeliness of data access.

More specifically, a comparative study will be performed by comparing the proposed prototype with the existing system, with respect to healthcare quality metrics. A set of metrics as well as a suite of healthcare workflows and scenarios will be defined, jointly by the team and the medical staff in the partner medical institutions. Example metrics include the duration, cost, and throughput of a healthcare workflow; error rate in a data collection/retrieval session; timeliness (response time) of first aid; and more subjective metrics such as the value and usefulness of data at hand. Feedbacks from this evaluation will help in improving the usability and performance of the prototype.

This research funding will allow all these team efforts to accelerate and bring the intellectual merits to reality. Accompanied by the education and outreach plans, we expect to have substantial efforts underway to improve the quality of healthcare.