Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations

Yaorong Ge,[1] David K Ahn,[1] Bhagyashree Unde,[1] H Donald Gage,[2] J Jeffrey Carr[2]

[1]Department of Biomedical Engineering, Wake Forest School of Medicine, Winston-Salem, North Carolina, USA
[2]Department of Radiology, Wake Forest School of Medicine, Winston-Salem, North Carolina, USA

Correspondence to
Dr Yaorong Ge, Department of Biomedical Engineering, Wake Forest School of Medicine, 2nd Floor MRI Building, Medical Center Blvd, Winston-Salem, NC 27157, USA;
yge@wakehealth.edu

Received 6 June 2012
Accepted 21 July 2012
Published Online First
11 August 2012

ABSTRACT

Background Current image sharing is carried out by manual transportation of CDs by patients or organization-coordinated sharing networks. The former places a significant burden on patients and providers. The latter faces challenges to patient privacy.

Objective To allow healthcare providers efficient access to medical imaging data acquired at other unaffiliated healthcare facilities while ensuring strong protection of patient privacy and minimizing burden on patients, providers, and the information technology infrastructure.

Methods An image sharing framework is described that involves patients as an integral part of, and with full control of, the image sharing process. Central to this framework is the Patient Controlled Access-key REgistry (PCARE) which manages the access keys issued by image source facilities. When digitally signed by patients, the access keys are used by any requesting facility to retrieve the associated imaging data from the source facility. A centralized patient portal, called a PCARE patient control portal, allows patients to manage all the access keys in PCARE.

Results A prototype of the PCARE framework has been developed by extending open-source technology. The results for feasibility, performance, and user assessments are encouraging and demonstrate the benefits of patient-controlled image sharing.

Discussion The PCARE framework is effective in many important clinical cases of image sharing and can be used to integrate organization-coordinated sharing networks. The same framework can also be used to realize a longitudinal virtual electronic health record.

Conclusion The PCARE framework allows prior imaging data to be shared among unaffiliated healthcare facilities while protecting patient privacy with minimal burden on patients, providers, and infrastructure. A prototype has been implemented to demonstrate the feasibility and benefits of this approach.

INTRODUCTION

The ability to share patient medical records across providers of different organizations and locations has tremendous benefits for patients and the healthcare system.[1–3] Medical imaging is an important category of medical data with unique characteristics. It is among the most expensive and fastest growing procedures owing to continued improvement of imaging technologies. Its growing volume of data is significantly larger than that of other clinical data. It is widely expected that sharing medical imaging data across healthcare enterprises will improve the quality of care and reduce healthcare cost.[4]

Since 2005, regional health information organizations (RHIOs) and health information exchanges (HIEs) have been established to enable sharing of essential medical information. To date, the majority of RHIOs/HIEs are sharing only summary medical data. Recent studies show the considerable benefits of health information sharing.[5–7] To further enable data sharing across RHIOs/HIEs, a National Health Information Network (NHIN) is being developed and is undergoing regional testing.[8]

Besides the established RHIOs/HIEs, healthcare facilities currently rely on patients to manually transport medical imaging data to other facilities using physical media such as CDs and DVDs. Typically, a patient goes to the source imaging facility, requests a copy of the imaging data, signs the necessary paperwork for consent and other agreements, receives a copy of the imaging data on CDs or DVDs, and then carries these media to the new facility at the next appointment. The new facility retrieves and views the imaging data, and may keep part or all of the imaging data for future reference. Experience in the past few years has shown that this manual process is burdensome and prone to error for both patients and providers.[4] For example, the source imaging facility may copy a wrong study to CDs or the patients may misplace their CDs. The requesting provider may not be able to load the CDs or may link the outside study to a wrong patient record after it is imported. On the other hand, this manual process has the advantage that the consent and regulatory procedures are well established. Patients are in full control of the sharing process and can protect their privacy. Furthermore, the sharing facilities do not need prior agreements to exchange data: it is the patient who binds the facilities together by identity matching, consent, and other regulatory requirements.

In this paper, we describe an image sharing framework that fully leverages patient participation to overcome some of the drawbacks in existing HIE approaches.

BACKGROUND

Overview

Methods for data sharing can be categorized according to who coordinates the sharing: *organization-coordinated* versus *patient-coordinated*; and according to the way in which data are organized: *centralized* versus *distributed* data storage.

In the *organization-coordinated* sharing approach, healthcare organizations form a sharing network with pre-negotiated policies and methods. Users of the sharing network can access patient data from any participating organization at any time as long as they follow the network's access policies. Patients provide broad consent but are, thereafter, not involved in the sharing process. In contrast, the

patient-coordinated approach does not require sharing organizations to have direct relationships. It is the patient who coordinates the transfer of data from the source institutions to the destination institution and, in doing so, is able to directly control who has access to what data and, thus, can more carefully protect his or her privacy.

For data storage, most sharing approaches adopt the *centralized* data strategy, which replicates patient data from all participating institutions to a central data repository. Data sharing is achieved by accessing the central data repository without the involvement of source institutions. In the *distributed* data strategy, the source institutions maintain the original datasets without such replication. Data sharing is achieved by querying and requesting data directly from each source institution at the time it is needed. In order to enhance the performance of this strategy, a central repository of metadata that indicates the location, type, and other characteristics of the patient data is usually maintained so that the record locator services can efficiently identify all the source institutions with the desired datasets.

Sharing of non-imaging data

For non-imaging data, most approaches use an organization-coordinated and centralized data strategy.[9–11] McMurry *et al*[12] proposed a distributed architecture for data sharing in NHIN. They listed five important factors for distributed information architecture: (1) distributed storage; (2) institutional autonomy; (3) oversight and transparency; (4) access control based on investigator needs and institutional policies; and (5) self-scaling architecture.

In recent years, patient-coordinated data sharing has been investigated with the advent of patient health record (PHR) systems.[13 14] Patients may enter data manually or authorize healthcare organizations to submit data electronically to the PHR. For PHRs that connect multiple institutions, once the data are collected, patients may give their physicians access to their data during future visits.

Sharing of imaging data

Both organization- and patient-coordinated methods for general medical data sharing also apply to imaging data. However, the distributed storage strategy is preferred owing to the large amount of imaging data. The Integrating the Healthcare Enterprise technical framework defines the cross-enterprise document sharing for imaging integration profile[15] for organization-coordinated, distributed image sharing. Grid-based architecture has also been proposed for distributed image sharing.[16 17]

More recently, centralized storage strategies have been adopted for organization-coordinated and patient-coordinated image sharing by some exchanges using cloud-based technologies.[18] These approaches are mostly ad hoc and transient: a provider uploads an image to the cloud, sends the universal resource locator (URL) to the other provider, then the other provider uses the URL to view or download the image. Owing to the large size of the imaging data, they are usually deleted from the cloud after a limited time (eg, 1 month).

The cloud-based approach has also been proposed to enable patient-coordinated image sharing using PHRs. Mendelson described a recent effort by the Radiological Society of North America to enable image sharing using a cloud-based PHR.[19]

Challenges

For organization-coordinated sharing, the biggest challenges are how to protect patient privacy, ensure patient safety, and comply with federal and state laws and institutional policies.[1 2 5 20–26] The current design of RHIO/HIE and NHIN has recently provoked criticism and debate among patient advocates and privacy communities.[25–28] Related to these issues are institutional trust and liability concerns.[22 29] Additionally, linking patient records from multiple institutions, the Master Patient Index (MPI) problem, is also a major challenge.[23]

Patient-coordinated sharing can theoretically overcome many of the patient privacy and safety challenges facing the organization-coordinated approaches.[30] However, it also faces a number of significant challenges, especially for the sharing of imaging data using existing PHR models. These challenges include the burdens on patients, providers, and infrastructure.

METHODS

Overview

Our framework aims to provide an image sharing network that is scalable nationwide and is effective in protecting patient privacy and safety. The overall design is based on five fundamental principles that address drawbacks in existing solutions:

1. Different clinical situations and cases may require different image sharing approaches. The overall network should support both approaches so that the most appropriate method can be used.
2. Physician workflow must be respected and remain efficient and effective to ensure best quality of care.
3. Patient involvement should be fully leveraged to simplify design, but patient burden must be minimized to achieve wide adoption.
4. Patient control can be achieved without necessarily requiring patient access to actual data.
5. Imaging data should be maintained by the source imaging facilities and exchanged only when needed in order to minimize storage and bandwidth requirements.

Architecture

As shown in figure 1, the proposed image sharing framework is logically composed of a Patient Controlled Access-key REgistry (PCARE) master server and a network of PCARE facility servers, one at each participating facility (note that each server may require multiple physical or virtual servers). In the following sections, we will describe the major components of the master and facility servers.

PCARE master server

Patient Controlled Access-key REgistry

A core component of the master server is PCARE (see figure 2A). This is the critical design feature that sets our framework apart from existing patient-coordinated sharing frameworks such as PHRs. Instead of dealing with actual clinical data as in a PHR, PCARE is a collection of access keys or secure tokens that uniquely represent clinical datasets. These unique access keys are generated by a healthcare imaging facility upon patient authorization to provide a secure electronic conduit to the actual dataset.

Each access key is a token that can be used to redeem the corresponding dataset. It contains a limited and specified number of attributes, such as the patient's name, date of birth, and the patient's unique identifier at that facility (commonly referred to as a "medical record number"), in addition to metadata describing the dataset. The access key and accompanying patient metadata are encrypted and digitally signed so that only the patient and this facility can decrypt and authenticate the content. Furthermore, each access key also contains URLs that specify links to the facility that issued the key. These

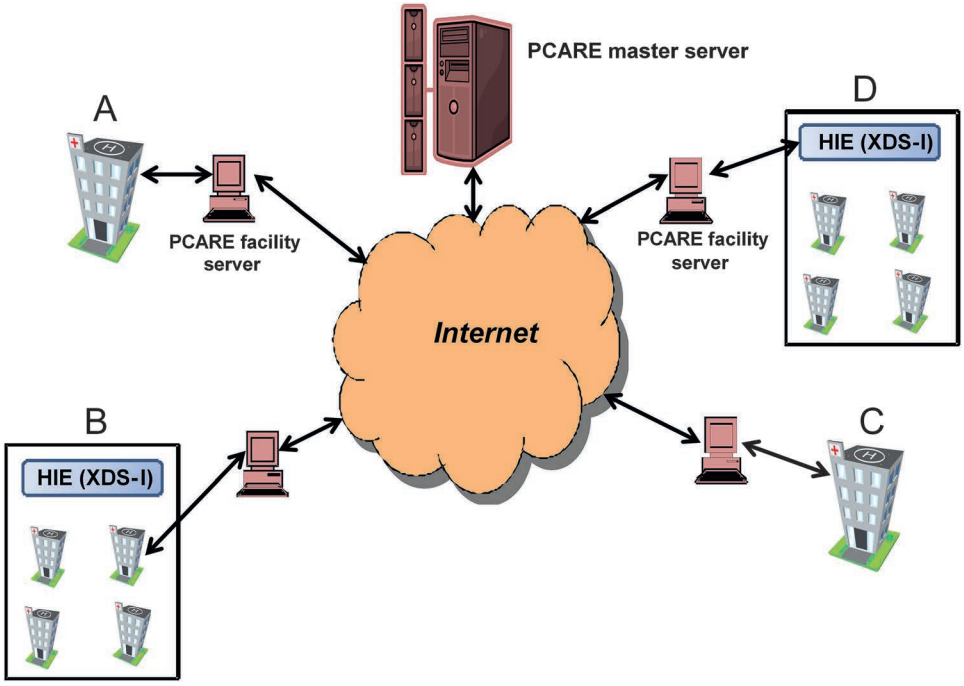

Figure 1 Overall architecture of the Patient Controlled Access-key REgistry (PCARE) patient-coordinated image sharing network. Each node of this network may be an independent healthcare enterprise (A, C) or an organization-coordinated image sharing network such as a health information exchange (HIE; B, D).

facility-specific URLs provide the links to services where the actual clinical data, in this case medical imaging data, can be obtained. To ensure strong security, the facility must update the access key periodically or whenever relevant information changes—for example, when a facility's URLs change. For finer control of access, multiple access keys may be generated for each patient to allow access to different parts of a patient's health record.

Patient-linked MPI

Another critical component of the PCARE master server is the MPI. As discussed previously, the MPI links together patient identities that may be different at different healthcare facilities. In organization-coordinated sharing networks, MPI is established by comparing demographic information in existing records. In the proposed framework, we fully leverage patient participation in their healthcare process by enabling patients to establish the linkage between their local identity and the PCARE identity as a part of their normal registration or check-in process. The MPI created through such physical verification processes eliminates major sources of error in conventional MPI linkage systems.

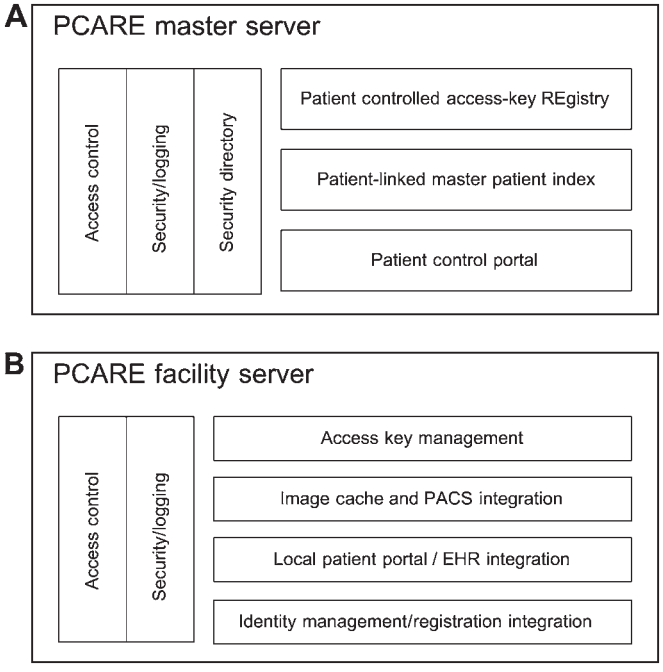

Figure 2 System architecture. (A) Major components of the Patient Controlled Access-key REgistry (PCARE) master server. (B) Major components of the PCARE facility server. EHR, electronic health record; PACS, picture archiving and communications system.

Patient control portal

The third major component of the master server is the patient control portal. We note the difference between a patient control portal and a patient access portal. Most patient portals, including PHRs, are access portals as they give patients direct access to their health data. However, we believe that access to the actual data is not necessary for patients to control their privacy in a data-sharing network. The access keys in PCARE provide metadata information about the type of studies that are sufficient for patients to make their sharing decisions. Therefore, our patient portal is called a *patient control portal* to emphasize that in the portal patients are admitted to access keys rather than actual health data, and that patients control the exchange of health data rather than view or manipulate the actual content of health data.

In addition to access keys, each PCARE account in the patient control portal maintains an audit log of how and when the keys are used for health data exchange. The audit history is important for meeting security and privacy requirements of the Health Insurance Portability and Accountability Act and other local regulations. It also provides useful information enabling patients to manage their own care. For example, the patient will know who has permission to access their information and which facilities and providers have actually exchanged information and when.

Facility directory, access control, and security/logging

The facility directory contains a list of all facilities in the sharing network, including information about the facility server in each

participating institution. The access control module is responsible for authenticating and authorizing access to all the components in the master server. The security/logging module is responsible for securing communication channels between the servers and logging activities by various server components as well as users.

PCARE facility server

The facility server is the gateway for each participating institution. Each facility server corresponds to one node in the PCARE network that represents one institution.

Access key management

As shown in figure 2B, access key management is a core component of the facility server. It is responsible for generating, submitting, updating, and verifying access keys based on data received from the local facility's electronic health record (EHR) system, radiology information system (RIS), and/or picture archiving and communications system (PACS) and from the master server.

Image cache and PACS integration

To the local facility PACS or image viewers, this cache serves as the image source that contains images from external sites. One important function that this component performs is the translation of patient identifying information from the source imaging facility to the local imaging facility. It is also the image consumer that receives images from the local facility and extracts image metadata for access key generation. To all other external facilities, it serves as the gateway to the images stored at this local facility. After the access keys are obtained and verified, this component handles the retrieval of imaging data from the local facility and the transmission of those data to the image cache of the requesting facility server.

Local patient portal/EHR integration

Reports for imaging studies are often stored separately from the images themselves at local facilities. The former in an EHR or RIS while the latter is a PACS. With the recent meaningful use requirements of the Health Information Technology for Economic and Clinical Health Act, most healthcare facilities have implemented patient portals as either a part of the EHR system or as an independent component to provide clinical data, including imaging results, to patients. The local patient portal/EHR integration component establishes integration with IT systems of the local facilities for two main data elements: patient imaging reports and patient identities in local EHR and/or patient portal.

Identity management/registration integration

This component may be an independent module of the facility server or part of the EHR/patient portal integration. The purpose of this component is to enable registration staff to provide linkage between a patient's local identity and the PCARE identity via the standard registration process. This linkage is used to maintain the MPI in the master server.

Access control and security/logging

Access control and security/logging ensure safety of patient information and compliance of policies and regulations at the facility server level. The design of these components should enable patients to handle authentication and authorization in various ways that minimize patient burden, including verbal requests, phone, fax, access card, and online mechanisms. The security/logging component ensures that data transfers among all services within and across all facilities are authorized and secure. Additionally, this module allows local facilities to define business rules that enforce specific exchange policies for certain user, data, and facility types.

Prototype implementation

We have implemented a prototype of the proposed PCARE framework by adopting and extending existing open-source technologies and by developing core components for access key management and patient control mechanisms. Most components are written in the Java language and are integrated using web services-based application programming interfaces.

Access key management and PCARE registry

The data structure and algorithms for access key management are central to the success of this framework. In this implementation, the access keys are implemented as *tokens*, in the spirit of the tokens used in the security assertion markup language standards.[31] As shown in figure 3A, the basic design of a token contains important attributes, such as ID, type, and recipient facilities, and a link to parent tokens.

This token data structure provides sufficient flexibility to enable complex use cases of patient control and data exchange needs. This implementation uses three types of tokens:

Access tokens record parameters for patient authorization: who can or cannot access what data elements during what time period and under what conditions. A chain of access tokens provides the entire history and details of a patient's authorization decisions.

Resource tokens capture metadata related to their corresponding imaging data. A chain of tokens can further capture the update history of the imaging data.

Request tokens refer to access tokens and provide all the information that is needed by the source imaging facility to verify patient authorization and extract the specific datasets for exchange.

Samples of these tokens are illustrated in figure 3B–E. Here, the access token in (figure 3B) is created for future imaging data to be acquired at a facility while the access token in (figure 3D) is created for existing imaging data to be exchanged. Also note that the access token in (figure 3B) has a scope of "visit ID", illustrating the possibility of applying this token to only those imaging data that are acquired during a specific visit. The request token in (figure 3E) refers to one access token (ID: 1). It can also refer to multiple access tokens.

The PCARE card-based kiosk user interface

To minimize patient burden, we have developed a card-based user interface for easy authorization of data sharing by patients in most clinical situations. Credit cards, bank cards, insurance cards, and various other cards permeate everyday lives and the PCARE card is similar to a credit card. It stores identifying information that allows a patient to initiate image sharing control at a participating facility by swiping the card. A prototype user interface is shown in figure 4A. Here a laptop acts in place of a touch screen automatic teller machine style kiosk that allows either the patient or a facility staff to control image sharing.

Once the identity is established, the patient is given simple choices to control image sharing. As shown in figure 4B,C, the prototype implementation first asks the patient to decide how to manage images at the current facility and prior images stored at all other facilities. After confirming the selections, the patient can print the consent statement for future reference, as shown in figure 4D. At the same time, the PCARE facility server

A

Token
+ID
+Type
+Issue date
+Duration
+Issuing facility
+Issuing user
+Recipient facility(-ies)
+Recipient user(s)
+Context
+Access control
+Manifest
+Parent token
+Routing information
+Signature(s)

B

Sample Access Token for Patient with Pending Studies : Token
ID = 1
Type = access
Issue date = 11/1/2010
Duration = 60 days
Issuing facility = WFU
Issuing user = John Doe
Recipient facility(-ies) = PCARE
Recipient user(s) = <authorized>
Context = scope: visit, ID: 23456
Access control = Permit
Manifest = <none>
Parent token = <none>
Routing information = PCARE
Signature(s) = <binary signature>

C

Sample Resource Token for a Study created after Patient grants access : Token
ID = 2
Type = resource
Issue date = 11/5/2010
Duration = 5 years
Issuing facility = WFU
Issuing user = <inherit>
Recipient facility(-ies) = <inherit>
Recipient user(s) = <inherit>
Context = Scope: DICOM.Study, UID: 1.3.6.1.4.1.9328....
Access control = <inherit>
Manifest = Nested list of Study UID(s), Series UID(s), Instance UID(s), etc.
Parent token = 1
Routing information = <inherit>
Signature(s) = <binary signature>

D

Sample Access Token for Patient with Existing Studies : Token
ID = 3
Type = access
Issue date = 12/1/2010
Duration = <until revoked>
Issuing facility = WFU
Issuing user = Jane Doe
Recipient facility(-ies) = PCARE
Recipient user(s) = <authorized>
Context = Scope: Manifest
Access control = Permit
Manifest = Nested list of Study UID(s), Series UID(s), Instance UID(s), etc.
Parent token = <none>
Routing information = PCARE
Signature(s) = <binary signature>

E

Sample Request Token to retrieve an existing Access Token and its attached Resources : Token
ID = 100
Type = transfer
Issue date = 1/15/2011
Duration = 4 h
Issuing facility = LEXMEM
Issuing user = John Doe
Recipient facility(-ies) = PCARE
Recipient user(s) = <none>
Context = Scope: Access Token, ID: 1
Access control = <none>
Manifest = Optional nested list of requested study UID(s), series UID(s), instance UID(s), etc
Parent token = <none>
Routing information = PCARE
Signature(s) = <binary signature>

Figure 3 The access key is implemented as a set of attribute-value pairs known as a token. (A) All tokens have the same general structure; the "parent token" field allows a chain of tokens to be constructed; (B) and (D) the access token is issued and digitally signed by the patient and provides the permission to retrieve patient health data specified by one or more resource tokens; (C) the resource token is issued and signed by the imaging source facility that references the actual patient health data stored at the facility; (E) the request token is issued by a requesting facility to retrieve the health data specified by one or more access tokens from the imaging source facility.

immediately begins the process of requesting and transferring the authorized images from other facilities to the current facility for sharing with local physicians. This consent statement also enables the PCARE facility server to generate tokens for the authorized local studies and forward them to the PCARE master server for future sharing.

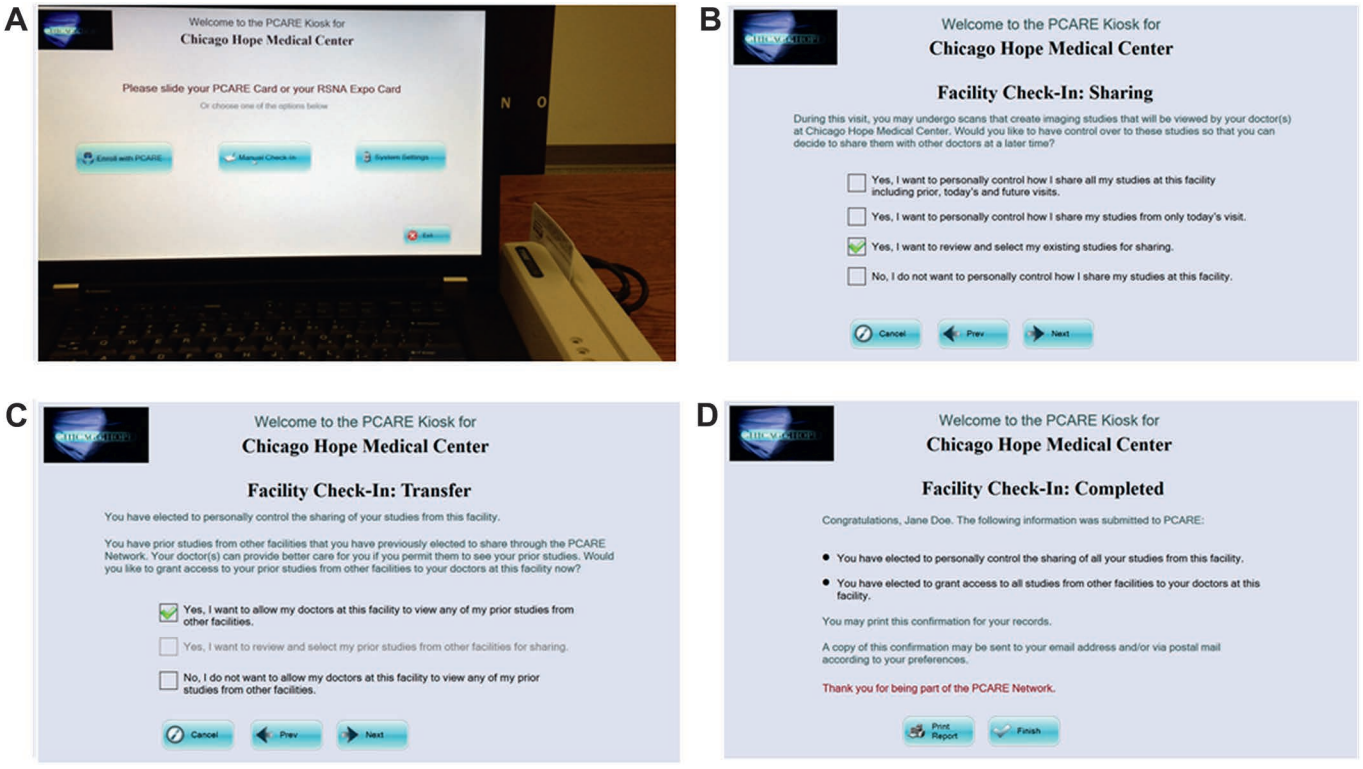

Figure 4 Patient Controlled Access-key REgistry (PCARE) card-based kiosk user interface. (A) In this pilot implementation, the kiosk is simulated with a laptop interface. A magnetic card reader is attached to the laptop computer. (B) After user authentication with a swipe of card and entering a PIN, the patient is asked to choose whether to enable sharing of the images at the current facility. (C) The next screen prompts the patient to determine whether the prior images from other facilities should be shared with the current facility. (D) Finally, the patient's selections are displayed in a consent report that can be printed for future reference.

RESULTS

The PCARE prototype has been implemented at Wake Forest Medical Center (WFMC), Winston-Salem, North Carolina, USA to assess the feasibility and performance of patient-controlled image sharing. The feasibility study involved one PCARE master server and one PCARE facility server deployed at WFMC and another PCARE facility server deployed at Lexington Memorial Hospital (LMH), a small community hospital in Lexington, North Carolina, USA. For maximum security, all servers were situated between the first and second firewalls inside the demilitarized zone with a small number of dedicated ports opened for network communications. Communication between the servers was over the internet but secured with the transport layer security protocol. The feasibility test was conducted over a 1-week period to ensure that, given patient permission, (1) tokens were successfully generated at local facility servers and submitted to the PCARE master server; and (2) images were successfully transferred between the two hospitals that independently maintained their own design of firewalls and security policies.

Next, a performance test was conducted to study the type of imaging studies that can be effectively exchanged between the two hospitals using their existing network infrastructure. Imaging studies of various modalities and sizes were exchanged over the PCARE network, and their transfer times were logged. As expected, the transfer times rose linearly with the size of the datasets and were limited by the available internet bandwidth.

A second performance test was conducted to exchange imaging studies between WFMC and a "simulated cloud hospital" (SCH). The PCARE facility server for SCH was deployed in a virtual machine in a commercial internet cloud hosting provider located in Newark, New Jersey, USA. Communication between WFMC and SCH was secured with a virtual private network connection.

Figure 5 illustrates the image transfer rate for both performance tests (WFMC-LMH in red and WFMC-SCH in blue). Notice that, even with the existing infrastructure of a small community hospital, the PCARE network can transfer more than 500 MB of imaging data (ie, more than 1000 CT images) in <10 min, which is a reasonable waiting time for typical clinical situations. Hospitals with a more modern infrastructure (SCH) will be able to transfer twice as much data during the same waiting period.

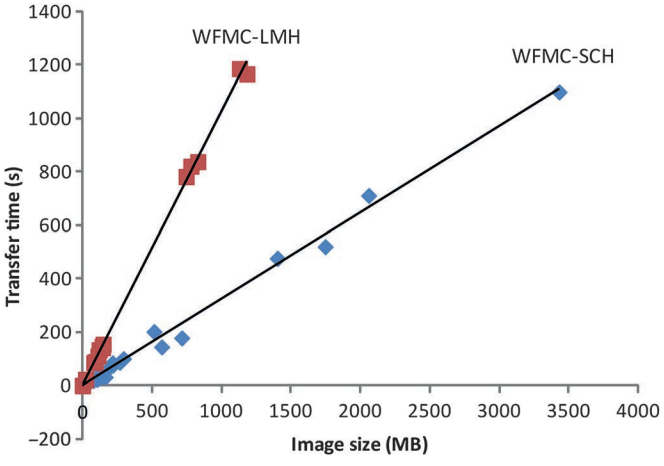

Figure 5 Image transfer speed at two pilot testing locations. The blue markers are between WFMC and SCH (a simulated larger hospital); the red markers are between WFMC and LMH (a small community hospital). Notice that the time increase fairly linearly as the image size increases. But even in a small community hospital, the Patient Controlled Access-key REgistry (PCARE) system can transfer more than 500 MB (or 1000 CT images) of data within 10 min, which is within a reasonable waiting time in most clinical situations. LMH, Lexington Memorial Hospital; SCH, "simulated cloud hospital", WFMC, Wake Forest Medical Center.

DISCUSSION

Conceptually, the proposed framework is a network of networks, similar to the designs of proposed NHIN[32] but with a fundamental difference: while NHIN uses only organization-coordinated sharing, our framework adopts patient-coordinated sharing at the higher levels while allowing the lower levels to be either independent facilities (figure 1A,C) or organization-coordinated sharing networks (figure 1B,D). We believe this hybrid sharing strategy achieves the best balance between physician workflow efficiency and patient privacy protection. By facilitating explicit patient consent and authorization for each specific sharing of imaging data across organization, network, or even state boundaries, this framework dramatically simplifies the problem of reconciling differing regulations, policies, and laws governing data sharing.[2 22 33]

Image sharing can be viewed as an access control mechanism for outside images. From this perspective, the key difference between our framework and existing access control frameworks is that we treat the problem of accessing outside data as uniquely different from accessing data within an enterprise. The conventional policy-based and role-based access control mechanisms work well within an enterprise or HIE.[34] However, they become increasingly complex and difficult to reconcile as data from multiple independent organizations are accessed.[22] Our framework uses different mechanisms to tackle these two different access problems which (1) require direct patient authorization to move data across enterprises; and (2) rely on conventional policy-based access control to access data within the enterprise. In essence, our framework automates the manual, patient-coordinated data exchange process that has worked successfully in practice.

The proposed framework does not deal with physicians' concerns or reservations about using outside images. Addressing these concerns will require standardization of image acquisition, quality assurance, and image interpretation protocols. It will also require mature legal, regulatory, and financial frameworks for cross-enterprise data sharing.

We also note that the consent languages used in the prototype implementation are for feasibility testing only. In a commercial implementation, the messages displayed and printed for patients should comply with, and adapt to, federal and state laws and institutional policies. For example, an informed consent form must be presented to, and signed by, patients before they are enrolled into the PCARE network.

Beyond image sharing, the PCARE framework can be used to implement federated and virtual shared EHR systems[35 36] with strong protection of patient privacy. A conceptual difference between PCARE and the virtual shared EHR system proposed by Bergmann, *et al*[35] is in the handling of patient consent. As described previously, the PCARE framework distinguishes data access across and within enterprises, and accordingly adopts a two-level consent mechanism: consent for sharing data between two organizations versus consent for accessing data within an organization. This strategy is critical for managing the complexity of legal and policy differences across enterprises and local governments.

A comprehensive assessment of the effectiveness of the PCARE framework requires further development of the

proposed framework and a full implementation in a clinical setting. Both efforts are underway.

CONCLUSIONS

The PCARE framework enables the sharing of prior imaging data among unaffiliated healthcare facilities while protecting patient privacy and data confidentiality. The design of the PCARE network focuses on minimizing burden on patients, providers, and infrastructure, and on maximizing both patient and institutional control over the sharing process. A prototype of the PCARE framework has been implemented to demonstrate the feasibility and benefits of this approach.

Acknowledgments We thank the anonymous reviewers for their insightful suggestions. This work also benefitted from discussions with Drs Thomas Arcury, Ha Nguyen, Annette Johnson, Joanne Sandberg, and Wenke Hwang.

Contributors YG and JJC were responsible for all aspects of this work, including conceptualization, design, and data analysis and interpretation. DKA and BU performed design, implementation, testing, and data acquisition. HDG focused on data acquisition, analysis, and interpretation. All authors participated in the writing and editing of the manuscript.

Funding This work was supported by the NIH/NIBIB grant 5 RC2 EB011406.

Competing interests None.

Ethics approval Ethics approval was provided by Wake Forest institutional review board.

Provenance and peer review Not commissioned; externally peer reviewed.

REFERENCES

1. **Kuperman GJ.** Health-information exchange: why are we doing it, and what are we doing? *J Am Med Inform Assoc* 2011;**18**:678—82.
2. **Vest JR,** Gamm LD. Health information exchange: persistent challenges and new strategies. *J Am Med Inform Assoc* 2010;**17**:288—94.
3. **Unertl KM,** Johnson KB, Lorenzi NM. Health information exchange technology on the front lines of healthcare: workflow factors and patterns of use. *J Am Med Inform Assoc* 2012;**19**:392—400.
4. **Flanders AE.** Medical image and data sharing: are we there yet? *Radiographics* 2009;**29**:1247—51.
5. **Gadd CS,** Ho YX, Cala CM, *et al*. User perspectives on the usability of a regional health information exchange. *J Am Med Inform Assoc* 2011;**18**:711—16.
6. **Ullman K.** Indiana data network provides one stop for inter-hospital connectivity. How an Indiana-based regional health data exchange helps CIOs save time and money. *Healthc Inform* 2010;**27**:32.
7. **Beckjord EB,** Rechis R, Nutt S, *et al*. What do people affected by cancer think about electronic health information exchange? Results from the 2010 LIVESTRONG electronic health information exchange survey and the 2008 Health Information National Trends Survey. *J Oncol Pract* 2011;**7**:237—41.
8. **Dixon BE,** Zafar A, Overhage JM. A framework for evaluating the costs, effort, and value of nationwide health information exchange. *J Am Med Inform Assoc* 2010;**17**:295—301.
9. **Donnelly J,** Mussi J, Parisot C, *et al*. Building an interoperable regional health information network today with IHE integration profiles. *J Healthc Inf Manag* 2006;**20**:29—38.
10. **Wilcox A,** Kuperman G, Dorr DA, *et al*. Architectural strategies and issues with health information exchange. *AMIA Annu Symp Proc* 2006;2006:814—18.
11. **Frisse ME,** King JK, Rice WB, *et al*. A regional health information exchange: architecture and implementation. *AMIA Annu Symp Proc* 2008;2008:212—16.
12. **McMurry AJ,** Gilbert CA, Reis BY, *et al*. A self-scaling, distributed information architecture for public health, research, and clinical care. *J Am Med Inform Assoc* 2007;**14**:527—33.
13. **Mandl KD,** Simons WW, Crawford WC, *et al*. Indivo: a personally controlled health record for health information exchange and communication. *BMC Med Inform Decis Mak* 2007;**7**:25.
14. **Mandl KD,** Szolovits P, Kohane IS. Public standards and patients' control: how to keep electronic medical records accessible but private. *BMJ* 2001;**322**:283—7.
15. **Mendelson DS,** Bak PR, Menschik E, *et al*. Informatics in radiology: image exchange: IHE and the evolution of image sharing. *Radiographics* 2008;**28**:1817—33.
16. **Zhang J,** Zhang K, Yang Y, *et al*. Grid-based implementation of XDS-I as part of image-enabled EHR for regional healthcare in Shanghai. *Int J Comput Assist Radiol Surg* 2011;**6**:273—84.
17. **Sharma A,** Pan T, Cambazoglu BB, *et al*. VirtualPACS—a federating gateway to access remote image data resources over the grid. *J Digit Imaging* 2009;**22**:1—10.
18. **Prestigiacomo J.** Taking it to the clouds. The image movement of Montana starts sharing images via cloud-based solution. *Healthc Inform* 2010;**27**:30, 32, 55.
19. **Mendelson DS.** Image sharing: where we've been, where we're going. *Appl Radiol* 2011;**40**.
20. **Adler-Milstein J,** Bates DW, Jha AK. A survey of health information exchange organizations in the United States: implications for meaningful use. *Ann Intern Med* 2011;**154**:666—71.
21. **Edwards A,** Hollin I, Barry J, *et al*. Barriers to cross—institutional health information exchange: a literature review. *J Healthc Inf Manag* 2010;**24**:22—34.
22. **Gravely SD,** Whaley ES. The next step in health data exchanges: trust and privacy in exchange networks. *J Healthc Inf Manag* 2009;**23**:33—7.
23. **Just BH,** Fabian DP, Webb LL, *et al*. Managing the integrity of patient identity in health information exchange. *J AHIMA* 2009;**80**:62—9.
24. **McDonald C.** Protecting patients in health information exchange: a defense of the HIPAA privacy rule. *Health Aff (Millwood)* 2009;**28**:447—9.
25. **McGraw D,** Dempsey JX, Harris L, *et al*. Privacy as an enabler, not an impediment: building trust into health information exchange. *Health Aff (Millwood)* 2009;**28**:416—27.
26. **Connors B,** Leipold J. The 42 CFR Part 2 and NHIN conundrum. *Behav Healthc* 2009;**29**:52—3.
27. **Sweeney L.** Privacy issues overlooked. *Mod Healthc* 2010.
28. **Rode D.** Building trust into the NHIN: key legislation can ensure the privacy of personal health information. *J AHIMA* 2005;**76**:18, 20.
29. **Goldstein MM.** Health information technology and the idea of informed consent. *J Law Med Ethics* 2010;**38**:27—35.
30. **Halamka JD,** Mandl KD, Tang PC. Early experiences with personal health records. *J Am Med Inform Assoc* 2008;**15**:1—7.
31. **SAML Tokens and Claims.** *MSDN Library*. 2012. http://msdn.microsoft.com/en-us/library/ms733083.aspx (accessed 3 Jan 2012).
32. **ONC-HIT.** *NHIN Architecture Overview*. 2010. http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11113_911643_0_0_18/NHIN_Architecture_Overview_Draft_20100421.pdf (accessed 1 Mar 2012).
33. **Stevenson C,** McDonnell S, Lennox C, *et al*. Share, don't hoard: the importance of information exchange in 21st century health-criminal justice partnerships. *Crim Behav Ment Health* 2011;**21**:157—62.
34. **Caumanns J,** Kuhlisch R, Pfaff O, *et al*. *Access Control. IHE IT-Infrastructure White Paper*. 2009. http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper_AccessControl_2009-09-28.pdf
35. **Bergmann J,** Bott OJ, Pretschner DP, *et al*. An e-consent-based shared EHR system architecture for integrated healthcare networks. *Int J Med Inform* 2007;**76**:130—6.
36. **Kalra D,** Lloyd D, Austin T, *et al*. Information architecture for a federated health record server. *Stud Health Technol Inform* 2002;**87**:47—71.