Sharing clinical documents in a national care provider network to support community-based medicine

Christian Lovis,
Stéphane Spahni,
Emmanuel Durand,
David Bandon,
Antoine Geissbühler
Service of Medical Informatics,
University Hospitals of Geneva,
Geneva, Switzerland

Correspondence:
Christian Lovis
University Hospitals of Geneva
Service of Medical Informatics
Integrated Electronic Patient Record Group
21, rue Micheli-du-Crest
CH-1211 Geneva 4
christian.lovis@hcuge.ch

Summary
One of the key factors in improving the quality of care in a community-based healthcare network is maintaining the continuity of care. Continuity of care implies the ability to take care of patients in a coherent and relevant manner. It depends heavily on the integrity of the information flow, especially where several care providers are involved. Promoting information flow in the very sensitive field of patient data may, however, come into conflict with the ethical and legal environment. We describe the implementation of a secure server, using a Swiss protected network via the Internet devoted to care providers and allowing the sharing of clinical documents in a very tight patient-care provider relationship. The patient can choose which documents will be made available to the care provider he selects, thus empowering his control over his own medical data. This is the first step in establishing a distributed, patient-controlled, virtual patient record (VPR). Virtual patient records provide a means of integrated access to patient information which may be scattered around different healthcare settings.

Introduction
With the rising cost of the healthcare system, gains in efficiency and growing quality concerns, the care dimension is increasingly viewed in a more global perspective, the continuum of the patient’s life. The electronic personal healthcare record has been recognised as a major tool for continuity of care, fostering closer involvement of the patient/citizen in the health care, prevention and promotion processes. As such, it has been considered a priority in the European Community for several years [1]. There is little doubt that many difficulties arise from poor communication between hospitals and general practitioners. This is further exacerbated by a lack of standard protocols for the preparation and dissemination of discharge summaries. Studies have clearly shown a decrease in inappropriate hospitalisations and rehospitalisations where proper transmission of discharge summaries was available [2]. Nowhere is this more evident than in the case of residents of aged-care facilities returning from hospital with radically changed medication regimens.

In 1997 the US Institute of Medicine (IOM) classified the major uses of the patient health record into two categories:

Primary uses
– Patient care delivery
– Patient care management
– Patient care support processes
– Financial and other administrative processes
– Patient self-management

Secondary uses
– Education
– Regulation
– Research
– Public Health and homeland security
– Policy support

According to the IOM (National Academies of Science press release, 7/31), electronic records should support:
– Physician access to patient information, such as diagnoses, allergies, lab results and medications;
– Access to new and past test results among providers in multiple care settings;
– Computer order entry;
– Computerised decision-support systems to prevent drug interactions and improve compliance with best practices;
– Secure electronic communication among providers and patients;
– Patient access to health records, disease management tools and health information resources;
– Computerised administration processes, such as scheduling systems;
– Standards-based electronic data storage and reporting for patient safety and disease surveillance efforts

In this respect, and in order to improve the quality of care, the IOM has started a project for building a model of a 21st Century Community Health Care System in Rural America. The study will make recommendations on an agenda for quality improvement in rural settings and identify the performance characteristics that models for 21st century community rural health systems should meet.
Sharing information

If they are to make sound clinical decisions, care providers require information. Unfortunately, their information needs are often not met [3]. This lack of information may result in inefficient care, duplicate actions and, subsequently, lower-quality care. For example, the possibility of displaying laboratory test results can reduce the number of redundant tests ordered, saving money and preventing unnecessary tests; in conjunction with pharmacy information, it can lead to significant adverse events reduction [4]. Access to electronic consults and patient consents can establish critical linkages and improve care coordination among multiple providers, as well as between provider and patient [3].

Communicating

Lack of communication between all stakeholders in a care relationship, including care providers and patients and their families, may contribute to the occurrence of adverse events [5]. Communication is critical to the delivery of quality health care, especially for patients with chronic conditions and patients with multiple providers in multiple settings needing careful coordination. In addition, it has been shown that good communication can help reduce cancer risks, incidence, morbidity, and mortality while enhancing quality of life across the continuum of cancer care [6]. However, although communication interfaces are well established for administrative data exchange, such interfaces for clinical data exchange are still beset by many problems. A shared and integrated health record, both within a setting and across settings and institutions, would be a major instrument in meeting the need for continuity of care. However, in Switzerland at least, this remains a long term goal.

Background

The Canton of Geneva is an urban area (282 km²) of Switzerland with a population of 440'000 and Geneva as its capital. The Geneva University Hospitals (HUG) is a consortium of hospitals, comprising more than 2'000 beds, approximately 45'000 admissions and over 450'000 outpatient visits each year. It is the only public and teaching care consortium of the state. The current clinical information system provides access to more than 2'000'000 medical documents online and all laboratory results, and stores about 13'000 new radiology images daily. The Geneva state is in the study phase of a large community-based care network which will include all public and private care providers as well as all citizens. This future network, named e-toile, will allow providers to share information in a peer-to-peer protected network in a distributed architecture with strong patient-care provider authentication. Electronic communication tools, such as e-mail and web messaging, have been shown to be effective in facilitating communication both among providers and with patients [7, 8].

The project

The project's goal is to be able to publish any computerised document produced in the HUG, including such documents as lab results or radiology images, to the private physician in charge of the patient, in compliance with Swiss and Geneva state law on the protection of private data, personal information and health care records. This means, for example, that security and integrity of communication must be ensured, that only those care providers formally designated by the patient can receive information, all transactions must be traceable and under the responsibility of an identified and authenticated authorised user. In addition, the project had to be feasible within a realistic time period, use existing infrastructure as far as possible and be economically viable.

Architecture

An overview of the architecture is given in figure 1. The first layer is the Internet browser and authentication process via the Access Control Server (ACS). This will provide a secure and authenticated connection. The server then acts as proxy to another server, the provider server, which can be located in a DMZ zone. In our case the document server and the authorised GPs list is located on a server of this kind. This server has no access to the intranet servers. The documents will be fed from the intranet servers, which hold the CPR, to the CPR component located in the document server. This architecture permits both the use of authenticated and secure connections and a strong firewall between intranet and Internet.

Health secured network

To enforce the requisite security level the project uses an existing secure communication network via the Internet. The Swiss healthcare protected
network, named HIN for Health Info Net, allows authenticated communications based on the principle of Public Key Infrastructure (PKI). HIN is a company owned mainly by the Swiss Medical Association and the Swiss Physicians’ Fund (CdM / AeK). Since 1996 HIN has operated its own secure infrastructure based on the ASAS (Arpage Security and Access System)\(^1\) implementation [9] of Virtual Private Networks (VPN) in association with encryption, authentication and access control. It thus implements various functionalities in a strongly secured core:

- Establishing a secure communication channel between a client application and a server application (i.e. an encrypted tunnel such as "HTTPS");
- Enabling secure authentication of the communication partners through the exchange and validation of certificates;
- Offering various mechanisms for limiting of access to controlled resources, such as closed users groups (CUG) or access control lists (ACL);
- Supporting S/MIME mechanisms for a reliable and safe exchange of e-mails.

ASAS is not only a security toolkit: it is also an implementation of a certificate authority. Indeed certificates used in the HIN infrastructure are issued by HIN itself. All certificates are validated before each use. The ASAS client requests this validation automatically each time it has to use a certificate. This ensures that no outdated or revoked certificate is used without the user’s knowledge.

The document server

The document server receives documents from the HUG’s computerised patient record. It is logically separated from the CPR by a secured communication layer between the intranet and the extranet. It can only be accessed by GPs who are authenticated in the ACS. This intermediate repository makes it possible to avoid any direct link between the Internet and the intranet.

Dealing with images

Radiological images can also be transmitted to GPs via the document server. To optimise performance we currently limit this feature to the most relevant images selected by the clinicians in the CPR. The selection and publication mechanisms rely on close integration between the CPR and a PACS (picture archiving and communication system). Moreover, we have arranged with our PACS commercial supplier\(^2\) to share the same data format, so that we can implement our own plugins such as a selection wizard. First, clinicians load images in the PACS image viewer, which is fully embedded in the CPR user interface. They then tag the relevant images to be transmitted using the image selection wizard (figure 5). The wizard inserts the images into a portable Adobe PDF document and this publishes them on the document server. We are now developing a more advanced solution based on image distribution using wavelet compression techniques. This solution will allow more advanced image display and manipulation capabilities.

Standards and formats

The technical layer is based on Internet standards such as IP, http, https and XML. Inside the HIN secured network, data communication encryption is performed using triple DES with 192 bit keys and users are authenticated through their X.509 certificate (based currently on 1024 bit RSA keys). To be able to guarantee the level of security, all encryptions and key management are performed by the ASAS software client, thus avoiding reliance on software with a potentially lower security level. The link between the HIN computing centre and the HUG server can be implemented using different security levels, ranging from an SSL tunnel to a private virtual or physical connection.

With the exception of the ASAS security layer client which needs to be installed, all software is that used for ordinary web browsing. Documents, reports, laboratory or any other non-


\(^2\) Supplier: Image Devices, division of Cerner company. Germany.
image-only documents are made available in Adobe PDF with standard security which does not allow editing. A certificate approach for the PDF is to be studied. In the present implementation, radiology images are exported from DICOM to JPG before being made available. We took this decision largely to allow transfer of images also for low bandwidth connections. A public domain DICOM viewer is being investigated and we hope that a tool of this kind will be available.

Operation
A GP wishing to access the HUG’s medical document server must be known and authenticated in the HIN secured network. Once known, the GP must register in the HUG care provider’s addressee list, where a manual check will be performed. Once the care provider has been approved, he will be made available in the potential addressee list of the document server.

On the other side, a HUG care provider who is logged into the CPR and has selected a patient with the correct access rights will see all addressees and a list of all documents available for this patient.

The physician at the University Hospital must select both the addressee and the documents specifically made available to this addressee with the formal agreement of the patient concerned (figure 2). Once validated, these documents will be available on the document server only to the care provider which has been selected (figure 3). The addressee can then select a document or an image and either view it direct (figure 4) or download it to its CPR.

All actions are traced on a central log server so that the patient can see at any moment which documents have been made available to what care provider, and what care provider has viewed which documents.

Conclusion
We have developed a document server that can be seen as a component of a virtual computerised patient. This component will provide access to documents which have been chosen by the patient for a care provider which has also been chosen by the patient, thus empowering the patient’s role. Virtual patient records (VPR) provide integrated access to patient information that may be scattered around different healthcare
settings. The core of this change is shaped by systems for computer-based patient records, which are part of local or regional networks, granting access to data in different information systems [10]. In principle, it should not matter where the patient data are located as long as data can be transferred to the physical location where patients and clinicians meet. Networking and electronic communication make it possible to create an environment that makes all systems where patient data reside act as one integrated, virtual CPR system from the user’s perspective. Internet-standard tools can be used to provide access for clinicians to the components of the electronic patient record held on multiple remote disparate systems. The patient record itself need not be physically located at one place, but is virtual and built dynamically in the right place, at the right time, with a content adapted the user [11, 12].

The main concern while implementing this document server has been to preserve the the patient’s private medical record and thus comply with Swiss legislation. The building of a VPR of this kind raises many ethical questions. Accordingly, maximum control has been handed to the patient. We hope that this model will be successful and be extended to other care providers in our community, thus making data sharing with respect for the patient a tool for achieving better quality of care.

References
12 Kay JD, Nurse D. Construction of a virtual EPR and automated contextual linkage to multiple sources of support information on the Oxford Clinical Intranet [In Process Citation]. Proc AMIA Symp 1999(1–2):829–33.