June 2005

A technological model to define access to electronic clinical records

A. Dalley
Illawarra Division of General Practice, Wollongong

J. Fulcher
University of Wollongong, john@uow.edu.au

D. Bomba
University of Wollongong, bomba@uow.edu.au

K. Lynch
Illawarra Division of General Practice, Wollongong

P. Feltham
Illawarra Division of General Practice, Wollongong

A technological model to define access to electronic clinical records

Abstract

This communication describes a functioning model that permits access to an electronic health record across a small number of providers resident in an Australian regional setting. Design criteria designated that provider access rights were to be assignable, revokable, transportable, and informable.

Publication Details

This article was originally published as: Dalley, A., Fulcher, J., Bomba, D., Kynch, K., Feltham, P. 2005, "A technological model to define access to electronic clinical records", IEEE Transactions on Information Technology in Biomedicine, June 2005 , Vol 9, No 2, pp. 289-290. ISSN: 1089-7771. Copyright IEEE 2005.

Communications

A Technological Model to Define Access to Electronic Clinical Records

Andrew Dalley, John Fulcher, David Bomba, Ken Lynch, and Peter Feltham

***Abstract*—This communication describes a functioning model that permits access to an electronic health record across a small number of providers resident in an Australian regional setting. Design criteria designated that provider access rights were to be assignable, revokable, transportable, and informable.**

***Index Terms*—Clinical knowledge architecture, consent, electronic health record (EHR), health-care document management, knowledge sharing between different healthcare groups, patient access, unique patient identifier (UPI), security, USB I-key.**

I. Background

There are around 500 diabetes patients registered with the Illawarra Division of General Practice (IDGP), who require regular consultations with their physicians [general practitioners (GPs)]. In order to facilitate the movement of these patients within the region's primary care health system, a mechanism whereby patients could remotely access their electronic health records (EHRs) was developed. In order to maintain continuity of informed care, patients were deemed to have the right to select which GPs, of those previously registered in the IDGP Diabetes Program, could be given permission to access their record. Remote, secure, and patient—accredited access to a central data repository was the chosen methodology.

The centralized diabetes database was updated on a weekly basis, using an automated uploading process of clinical diabetes-related information extracted from the medical director (MD) clinical software program running on the GPs' computers. Moreover, both patients and GPs successfully accessed the patient record via the IDGP website.

II. Field Trial

In order to test the validity of our technological model, we undertook a field trial involving 20 patients and their associated (6) GPs [1]. For the purposes of the trial, access was deemed to have four characteristics, namely: 1) assignable, 2) revokable, 3) transportable, and 4) informable. These characteristics mean that access could be both granted and revoked by the patient, and be available to a provider (GP) irrespective of where the patient was physically located.

Each GP and patient were matched with a 1024-bit randomly generated number. This number was subsequently installed on patient or practitioner transportable storage devices (USB I-Keys/memory sticks), and concurrently tabulated in patient and provider tables as the unique patient/provider identifier (UPI). GP I-Keys stored a single 1024-bit randomly generated UPI; patients' I-Keys stored multiple identifiers, these being a web server ID, a variable number of GP practice IDs (which increased as patients moved between practices), together with a local patient ID generated by the GPs desktop MD program.

The GP was prompted to insert their I-Key whenever their practice computer booted up. The GP's user identifier was stored in the computer's memory until required by the (automatic, periodic) uploading process. The software then went into background mode. A valid GP I-Key defined authorization for the GP to access the web-based patient record. Subsequent insertion of a valid patient I-Key activated that access to the specific patient record. This process replaced the existing user name/password access method, which permitted only *one* designated GP to ever access a given patient record. (However, patients were granted the right to access their own record externally on a user name/password basis.)

Whenever a patient I-Key was detected, a check was performed to determine whether that particular patient I-Key had previously been seen at this surgery. This was technically straightforward as both the patient's local ID and the recruiting medical practice's ID were stored on the I-Key. If the local ID could not be found on the I-Key, then a secure connection to the server was opened, and a transaction authorized using the GP's I-Key (still residing in memory from its earlier insertion), together with the current patient I-Key. If the two I-Keys were verified by the IDGP web server, it then transferred the patient's demographic record to the GP's computer. The local ID of this patient record was stored on the I-Key along with that practice's ID number, thus constituting a valid ID pair.

An on-screen prompt invited the GP to check whether any information had been added to the patient's record by other providers. If the GP accepted this invitation, the patient inserted their I-Key, thus completing the authorization process. A secure connection had, thereby, been established. The presence of new clinical information opened a web browser window allowing the clinician to view the patient's diabetes record on-line.

In the event of a communications failure, the GP was reliant on their existing clinical records. If the client software was unable to access the central server for uploading of new data, the information was stored, then forwarded at the next scheduled upload communication. The only impact on system functionality would be that information currently stored on the IDGP central database was unavailable for access through a web interface for the duration of the communications failure.

III. Technological Model

The technological model comprised the following:

1) a Microsoft SQL 7.0 database which holds the clinical records of the 20 participating patients;
2) an Apache 4.0 Web Server;
3) Rainbow I-Keys to store the 1024-bit identifier and less sophisticated IDs derived from the local surgery ID, as well as MD identifiers on the local MD database;
4) a user interface on the GP's computer, activated by the correct insertion of I-Keys into its USB port;

Manuscript received October 19, 2003; revised March 26, 2004 and October 11, 2004. This work was supported by the Australian Research Council under the Strategic Partnerships in Industry Research and Training scheme (Project C00001904).

A. Dalley, K. Lynch, and P. Feltham are with the Illawarra Division of General Practice, Wollongong NSW 2500, Australia.

J. Fulcher and D. Bomba are with the School of Information Technology and Computer Science, University of Wollongong, Wollongong NSW 2522, Australia (e-mail: john@uow.edu.au).

Digital Object Identifier 10.1109/TITB.2005.847143

5) a program to interrogate the GPs' computers for previously unutilized clinical information on trial patients and to transfer it to the IDGP server;
6) a Java applet situated on the trial's web-based login page to read information from the I-Keys;
7) provider and patient websites displaying the patient record and aggregated clinical data extracted from interrogation of all GP computers.

IV. System Security

The information stored on the I-Keys was protected (in the I-Key hardware) by a master password. I-Keys were only used to authenticate to the server; they performed no off-line function in our system.

The system logs website logins, website page views, and data uploads. Properly monitored, this enables an administrator to respond to inappropriate system usage.

V. Model Dependencies

Our technological model has a number of critical dependencies, as follows.

1) *Smart device*—Rainbow Technologies provided a USB I-Key Application Programming Interface [2], which was used in conjunction with C++ libraries to build custom software to perform functions such as uploading the UPI and formatting the I-Key.
2) *Accreditation of users*—A simple manual method of accreditation of users was utilized given the small number of participants [3]. IDGP authorized the GPs, all members of the organization, as known and trusted persons, while the GP's identified the patients as known and trusted persons. The patients were then authorized by IDGP administrative staff in that a person with an identified name vouched for by a trusted agent (the GP) was associated with a numeric identifier, which itself was associated with an electronic token (I-Key).
3) *Authentication*—Once the users were accredited and details stored in the IDGP database, this then became the central authentication database. All accesses to web pages were authorized by the web server utilizing this database.
4) *Lost keys*—During the project, no patients demised. In the event of a participant losing a key, the identifying number was marked as "revoked" on the central database. The number was not deleted so that it would be possible to track any future use of the missing key.
5) *Clinical software*—A further dependency was the MD clinical software. An independent clinical program was developed to store and download data in the case that a particular GP did not possess MD, however, this situation did not arise.

VI. Conclusion

There are two well-recognized core functions for smart tokens in the medical environment. The first is to act as a repository for clinical information. The second is to act as an identifier linking a card or token to a clinical record. This project focused on a third function—a smart token acting as a secure remote access mechanism to a patient's centrally stored clinical information. The use of codependant I-Keys provided a technically satisfactory means by which patients could grant contemporaneous access, revoke it, and transfer it to other accredited providers whose identity is known to the patient. This research is consistent with the Commonwealth of Australia's EHR initiatives involving UPIs, national practitioner authorization, and standard code sets. It provides the Australian health consumer with the possibility of consulting a range of providers, all of whom may have access to that consumer's health record wherever and whenever the patient (consumer) chooses.

References

[1] D. Bomba, J. Fulcher, and A. Dalley, "Lessons learnt from the UoW:IDGP smart_ID project," in *Proc. Health Informatics Conf. (HIC 2002)*, Melbourne, Australia, Aug. 4–6, 2002.
[2] (2002) About USB Smart Tokens and Smart Cards. Rainbow Technologies. [Online]. Available: http://www.rainbow.com/I-Key/index.html
[3] D. Bomba, J. Fulcher, and A. Dalley, "Construction of a diabetes database and pilot evaluation of ikey controlled GP-Patient access," *J. Info. Technol. Healthcare*, vol. 2, no. 5, pp. 1–11, 2004.