Implementing Security And Access Control Mechanisms For An Electronic Healthcare Record

Frank K. Ückert[1,2], Hans-Ulrich Prokosch[1] PhD

[1] Department of Medical Informatics and Biomathematics, University of Muenster, Germany
[2] Department of Pediatric Oncology, University of Muenster, Germany

ABSTRACT

Personal Electronic Health Records (EHR) have recently been published as one means to support patient empowerment and patient control over their personal health record.
The functionality of such an EHR may vary from a simple web-based interface for interactive data entry and data review up to a much more powerful system additionally supporting electronic data/document communication between clinical information systems of primary care practitioners or hospitals and even reminder based support for the empowered citizen, to actively take care of his health, based on relevant disease management programs. Since storage and communication of data in an EHR comprises sensible personal health data, each of those functions need specific security and access management requirements to be considered and implemented. In this article the most critical requirements for these aspects will be classified and respective mechanisms to provide secure data storage and communication as well as flexible access management functions will be presented.

INTRODUCTION

Electronic Patient Records (EPR) have been characterized by Waegemann as electronic collections of medical data for one individual patient, collected by different healthcare provider of the respective patient. Thus they already comprise provider-independent record collections. On the other hand the term Electronic Health Records (EHR) additionally puts emphasis on the active role of the empowered citizen in terms of patient involvement and control, and furthermore includes wellness and non-traditional health information.[1] In the context of the ongoing transformation of the physician/patient relationship slowly replacing the word 'patient', at least implicitly, by 'consumer'[2] and the increasing number of healthcare consumers demanding a more active role in their own care, such a personal health record can be seen as one major facilitator to support patient empowerment and patient control of their individual care process. While first evaluation results of patients accessing their personal medical records show their willingness to be empowered by such an access, their wish to really „control" their health records still varies.[3,4,5] Researchers agree in the conclusion, that security features need to be flexible and configurable, based on the needs and expectations of users and the actual functionality provided by the EHR.[3]

At Muenster University Hospital we have already initiated a project to design and develop an EHR in the year 2000 which has been called *akteonline*.[6] In contrast to many other EHR developments however, which limit their current functionalities to a password protected interactive patient access to their EHR via the Internet,[5] the concept of *akteonline* considers a much wider approach. It provides functions for

- a secure access by a citizen to his EHR via a standard browser. Currently data structures have been implemented for the storage of
  - basic personal data (e.g. contacts, next relatives, allergies, risk factors)
  - outpatient visits
  - inpatient hospital stays
  - medical conditions (history, diagnosis, treatment)
  - diagnostic examinations and results
  - immunizations
  - preventive care examinations
  - personal healthcare provider
- the provision of context-sensitive patient information
- electronic import/export of standardized clinical documents for the communication with healthcare provider
- reminder based disease management support

In accordance with those functionalities, security and access control functions have also been developed on different levels.

METHODS

First of all, on the basic technical level, *akteonline* has been split into two different logical databases which can be established on separated hardware platforms. The first database contains patient identification and demographic data (name, address, etc.) and links it to an internally generated patient ID, but no sensible clinical information. The second contains the actual clinical information, indexed by the patient's ID but without any personal data. Unallowed network access to both databases is prevented by a two-level firewall architecture. A citizen can not directly access one of those databases, but establishes access to the *akteonline* web server. Secure communication between users and the *akteonline* web server is established with the ssl-protocol, access to the *akteonline* databases is only established through secure connections between the web server and the databases. All data in the two databases are encrypted with symmetric keys. In order to support very granular access control mechanisms, separate data structures (e.g. medications, outpatient visits, inpatient visits, ...) in an individual's EHR are encrypted with different keys so that partial decryption for selected subsets can be supported. Thus, for every user a primary key table is implemented containing all the keys for each particular separate data structure. This key table itself is also encrypted with the clear text version of the user's password which is never stored within the EHR. In *akteonline*'s user authorization table only the version encoded by a one-way hash function is stored.

Access management

A flexible concept for the user to authorize persons or institutions to read and/or write data in his personal EHR is necessary. Following kinds of access are already implemented in *akteonline*:

Deputy function
The user is able to assign another user as a deputy with full control over his personal EHR. This deputy gets the choice of opening two different records, his own and the one he is deputizing for. All activity of the deputy – exactly like anybody else's – is logged and electronically signed, so the owner of the record can understand all the changes of his data. The deputy function makes it a lot easier to integrate minors or seniors, who are not able to use or who are not used to the internet.

Onetime access with TAN
With TAN (= transaction numbers) a user is able to give access to parts of his record to anybody for only one session. The principle of the TAN is similar to the one known from international online banking. After one usage the TAN is invalid. New TAN can be produced by the user whenever necessary. The user can adjust the type of authorization and the subsets of his record, which are made accessible through one particular TAN by a web interface using checkboxes.

Read access in emergency scenarios
If a patient wishes to provide read access to an "emergency subset" of his EHR, he can enable and define this within his record. For this purpose a default setting for the contents of the emergency subset (contact information and information about allergies, confirmed diseases and the list of actual medications) is provided, which may however be adjusted by the patient to his personal wishes. When this feature is enabled, an emergency TAN is created. The combination of web address, username and this emergency TAN printed on a small wallet card can be taken along by the patient and used by any other person in cases of an emergency for this patient.

Access for healthcare provider
Because healthcare provider can have an own login for *akteonline*, a user is able to select his healthcare provider and give him special authorizations for parts of his EHR. The access can be of reading or writing but not of overwriting nature. Data added by a healthcare provider is internally signed and cannot be changed by the user, yet he can delete them. Furthermore the assignment of access may also be granted for healthcare provider roles (e.g. pediatrician). This simplifies the procedure for the user to assign new and/or change healthcare providers, because the whole process may be pursued by simply adding a particular healthcare provider (e.g. physician) to a predefined role. In *akteonline* several medically useful roles are predetermined, which are meant as helpful suggestions and not as obligations.

Healthcare providers are able to access the EHR of a patient not only through the Web interface. Additionally electronic communication interfaces between the information system of a healthcare provider (e.g. a hospital information system) and the EHR have been realized. Standardised data interchange structures for these access channels were defined based on the Clinical Document Architecture (CDA).[7,8] The tool applied to structure the information is XML. Such an electronic communication can be performed totally transparent for the healthcare provider. There are two possible conditions for the acceptance of the data to be imported into *akteonline*:

- a general access authorization from the user for the respective healthcare provider. In this case the authorization is given on a basis of a triplet [P_{ID}, U_{ID}, authorization type] for each set of data. The P_{ID} stands for the identification number of the healthcare provider, the U_{ID} for the one of the user and owner of the EHR. The authorization type sets reading, writing or reading and writing authorization.
- a onetime access for a healthcare provider without own login name for *akteonline* through TAN. In this case the authorization is given through a triple [TAN, U_{ID}, authorization type].

Read access for reminder functions

Because data security is a major issue in implementing an EHR, the users′ clinical data are encrypted in such a way, that under normal conditions neither the system itself nor a system administrator has any access – not even a reading one – to the decrypted health records.

For the implementation of automated reminder functions however, which shall be applied to support disease management programs especially for patients with chronic diseases, access authorization needs to be granted by the user at least to those data items of his EHR which are part of the reminder logic. Since the activation of reminder modules is optional, the process of activating any reminder module is linked with an additional dialogue, explaining to the user which data items are required within this module and asking him to grant read access to those data for the respective system processes themselves.

The key table concept for EHR encryption

The data encryption principles of *akteonline* shall be illustrated by example scenarios.

In a first one the user "sampus" wants to be reminded of his regular preventive medical checkups. Therefore he selects and activates the appropriate reminder function. Transparently to the user a new key table for the system is created and encrypted again with the key of the reminder function, in which copies of user-keys for only the data sets which are necessary for the chosen function to work are deposited. In this case it would be birthday, sex, kinds and dates of the last checkups and the kind of insurance. Using those keys the reminder logic can always access the patient's data. If sampus decides to deactivate the reminder function the "borrowed" key copies will be removed.

In a second example the user sampus wants to give the healthcare provider "meddoc" read access to his lists of medications and healthcare providers. After selecting this option through the web interface only the two associated keys for decryption of those two data subsets are deposited in a new secondary key table of meddoc. This key table is encrypted by an automatically created password, which has to be given along to meddoc by sampus himself. The password is also stored as key in the primary key table of sampus. When meddoc logs in, his password is encoded by a one-way hash function and then compared with the encoded one already stored in the database. In case of a successful login meddoc's encrypted primary key table needs to be opened. The key to decrypt is the clear text version of the password, which is known only to the user or in this case the healthcare provider. Now *akteonline* informs him that sampus has granted him a new access right. For activating the access, the generated password has to be entered by meddoc. For security reasons this password is only usable by sampus and meddoc himself. After the activation, the password will become a key in the key table of meddoc, and can from now on be used for future access only to sampus' lists of medications and healthcare providers. All other parts of sampus' EHR are still encrypted and remain hidden.

The key table concept provides the necessary flexibility for realizing the different types of access management. The same principle is used for the other types of access. For example the TAN have their own key table which is filled by the user before giving a TAN away.

Coming to an even more granular view it is also possible to restrict access by encoding the datasets of a table with several different keys. This is necessary, if a user wants to give access e.g. for a TAN or a role in a very specialised way. A typical example is the view on psychiatric data (medication or visits), which usually is integrated into the rest of the data. Associated medications or inpatient visits may receive an own key. A healthcare provider or user of a TAN without this key is not able to see the designated sub data and will not even know about their existence.

The complex processes of administrating primary and secondary key tables are performed by the system. The user or healthcare provider only needs his password.

Signature and deletion of data

Each added set of data is internally being signed electronically. The signature serves like a stamp with the time and the username of the user who modified parts of the database. After signing a document (e.g. an electronic referral letter or an entry to the table of medications), which is done invisible for the one who enters or changes data, this document can not be altered anymore, not even by the owner of the record. It still can be deleted by the owner or his deputy. Making corrections as well as expressing a different opinion on signed entries is still possible. For this purpose an editable copy of the signed document is created, internally marked as a copy, and linked with the original document. The old version is still accessible and can still be seen. It is also possible to get a complete history of documentation.

To log information about the person and kind of authorisation who makes changes a logbook is being created by the system.

The function of deleting data is reserved for the owner or his deputy only. Usually deleting a set of data just changes an attribute from active to inactive. Especially for the medication this gets very useful when a user stops taking a drug and a healthcare provider wants to know at a later date if the user already had taken this drug and why it was deleted (or perhaps stopped being taken).

PROBLEMS AND SOLUTIONS

Token

The user login uses a combination of username and password. A password can be guessed, tried out or stolen. A combination of knowledge and possession would be more secure, so a possible extension for an EHR like *akteonline* may be the usage of a token. The display of a token shows a different number (tokencode) every minute, which looks like a random number but is calculated from the world time, and a unique secret 64Bit number in the token (seed). This seed is secured in a way that opening the token destroys the seed through power loss. The tokencode has to be entered during login along with the password. The use of a tokencode is only valid for one login during the minute the tokencode has been read.[9]

Loss of password

Because passwords are not stored in clear-text form, even an administrator is not able to recover a lost password. Setting a new one would not help, because opening the primary key table is only possible with the original password. To handle this problem, the user has to select a security question during the first time he works with *akteonline*. The answer of this question is encoded by the password hash function and then used for encrypting a backup key table. The key (hash of the answer) is stored in the primary key table. This way the primary and backup key table can be synchronized continuously. When loosing his password the user requests an email with his formerly selected security question. With the answer to that question and the username a login is now possible and the backup key table is used for creating a new primary one.

The condition for using this recovery function is making an actual email address available for the provider of *akteonline*. Changing the email address after loosing the password is not accepted.

Adding keys into the primary key table

Whenever new data is added to the EHR a new key has to be created and secured by the password of the user. The primary key table however is encrypted by the clear text version of the owner's password which is unknown to the system. Therefore, securing a new key during the session with this password is impossible. For this purpose every user has a "special"-key in his primary key table, which is only used to temporarily encrypt new keys being added to the key table. The new keys are also flagged for the system.

At the next login of the user, those newly added and flagged keys will be noticed, decrypted with the special-key and encrypted again with the clear text version of the user's password, which is accessible to the system only at this specific time.

DISCUSSION

Many researchers have reported the value for empowered patients to have access to their own patient information over the Internet.[3,4,5] Cimino and colleagues for example reported from a study in which both, patients and their caring physicians, believed that access to their personal health records enhanced the patient's understanding of their conditions and improved their communication with their physicians.[10] On the other hand, Kim and Johnson have recently analysed the functionality of eleven American Web sites promoting different electronic health records and found that currently available EHRs still demonstrate limited functionality.[5] One example for an extended EHR functionality has been described by Baorto and Cimino, with a prototype application which generated explanations of terms presented within an online pap smear report and linked to publicly accessible resources on the Web.[11] Ball and Lillis have additionally proposed the provision of software support for empowered patients (especially for patients with chronic diseases) to better manage their own disease.[2] Within clinical information systems such support is usually implemented by the means of electronic physician reminders, decision support functions for the clinician or electronic clinical guidelines. While all of those functions aim at the physician to be supported in their day to day decision making process, it still is a new concept to perform the next step towards patient decision support.[12,13] A further extension to an EHR which has been implemented by *akteonline* is, that the EHR may be applied as a communication medium to communicate clinical data (e.g. discharge letters) between hospital physicians and primary care physicians under the control of the patient.[6]

It is obvious, that more comprehensive functionalities in an EHR also need to be supported by a more complex access control management model. In such an approach completely new scenarios of establishing access rights and associating a user role with a physician have to be supported. In the above described model, it is no longer the system administrator who manages access control, but the patient himself. Thus, access control management functions need to be flexible enough to allow the configuration of very restrictive access rights (with specific restrictions to only small subsets of the EHR and even only one time access) as well as to establish quite comprehensive access to large subsets of the complete EHR. Such an access control model nevertheless must be easy to use and almost self-explaining, so that every patient can delegate access rights based on his personal needs and expectations and on the risk he is willing to assume.[3]

CONCLUSIONS

The model presented above has been implemented within the *akteonline* development and is currently under practical evaluation within a pilot project. As it has been described, we believe that it provides a comprehensive basis for stepwise further enhancements. The currently ongoing evaluation process will especially analyse, if the patients will be "empowered" enough to really use those functions and anticipate the new situation, where they themselves can really control whom they grant access to which subsets of their records. Furthermore it will be evaluated if the user interface for those features is easy enough to be handled by patients, so that the very rigid, but at the same time very flexible, safety model may in practice not be too burdensome to handle.

References

1 Waegemann CP. Current Status of EPR Developments in the US. In: Toward An Electronic Health Record ´99, Medical Records Institute. 1999: 116-118.

2 Ball M, Lillis J. E-Health: Transforming The Physician/Patient Relationship. International Journal of Medical Informatics 2001; 61: 1-10.

3 Masys D, Baker D, Butros A, Cowles KE. Giving Patients Access To Their Medical Records Via The Internet: The PCASSO Experience. J Am Med Inform Asocc. 2002 (9): 181-191.

4 Munir S, Boaden R. Patient Empowerment And The Electronic Health Record. In: Patel V. et al. (eds.) Proc Medinfo 2001: 663-665.

5 Kim MI, Johnson KB. Personal Health records: Evaluation Of Functionality And Utility. J Am Med Inform Asocc. 2002 (9): 171-180.

6 Ückert F, Görz M, Ataian M, Prokosch HU. Akteonline – Die Elektronische Gesundheitsakte Als Informations- Und Kommunikationsmedium Für Den Bürger. Proceedings of the Telemed 2001 Berlin: 30-37.

7 Health Level Seven, Inc. Clinical Document Architecture ANSI/HL7 CDA R1.0-2000. Internet: http://www.hl7.org (Access 02/01/14, 14:00 CET).

8 Dolin RH, Alschuler L, Beebe C et.al. The HL7 Clinical Document Architecture. J Am Med Inform Assoc. 2001;8: 552-569.

9 Internet: http://www.rsasecurity.com/products/securid/ (Access 02/02/20, 09:00 CET).

10 Cimino JJ, Patel VL, Kushniruk AW. What Do Patients Do With Access To Their Medical Records. Medinfo 2001;10(Pt 2): 1440-4.

11 Baorto DM, Cimino JJ. An "Infobutton" For Enabling Patients To Interpret On-line Pap Smear Report. Proc AMIA Symp 2000: 47-50.

12 Scott GC, Lenert LA. What Is The Next Step In Patient Decision Support? Proc AMIA Symp 2000: 784-8.

13 Chen Y, Wang SS, Cimino JJ. Linking Guidelines For Mammography To An Electronic Medical Record For Use By Patients. Proc AMIA Symp 2000.