A concrete Health Care Scenario

Jorge Cuellar

April 23, 2012

Abstract

1 General Context: Electronic Health Records (eHR)

Medical practices, hospitals and other Care Centers create, collect, and manage electronic health records (EHRs) for the purposes of treating a particular case and sometimes also for compiling the medical history of a patient.

Our approach is close to the so-called BMA-Model [1], which has been proposed to regulate the access to health records. In that model each health record has its own access control list, an approach which we consider to lack practicality. We regard our approach as an implementation or refinement of the BMA-Model. In ours, each record has an implicitly associated AC list, via some indirections which facilitate the understanding for patients and clinicians. There are also differences in the treatment of the sensitivity of EHRs, ours allowing for more flexibility. For other related work, see [2] and [3].

We propose to use the following terminology:

Electronic Health Record (EHR) is a single record of healthcare-*related* information. The EHR is the atomic unit of access control (a user is authorized to access records, not parts of records). Each single record is of a particular type, which can be of a wide variety of types, for instance,

- Patient demographics, including name, address, date of birth, health insurance number and the name of the treating doctor, and the details of the family doctor,
- Medical history, examination reports of health and illnesses,
- Medications, including side-effects and interactions, allergies, vaccination, and immunization status,
- Laboratory test results, radiology images or photographs,
- Record of appointments and billing records,
- Patients' directives, living wills, and health powers of attorney,

- Emergency contact info, etc.

The rules defining the access control criteria for an EHR will depend, among others, on the type of EHR. For instance, a highly sensitive record of a treatment for depression might be only available to his treating doctor (and perhaps a few others, on certain conditions), while a record of heart disease can be open to all staff, for the case of an emergency. In our scenario we will divide the EHRs in the four following:

Sensitivity Types The access control rules for EHRs depend on the "type" of EHRs. For this purpose, EHRs are grouped in "Sensitivity Types" (the types are not necessarily ordered in any particular way):

- *admin-EHR*,
- *emergency-EHR*,
- *normal-EHR*, and
- *restricted-EHR*.

EHRs that contain administration data are assumed to be of type *admin-EHR*, information that must be known by administrative staff for the case of an emergency are of type *emergency-EHR*, typical records are of type *normal-EHR*, and particular sensitive information (like so called psycho-sociological information, like a record of a treatment for depression) are of type *restricted-EHR*. The exact type of EHRs or medical information contained in those types is irrelevant for our purposes.

2 Scenario definition

We focus here on a rather prototypical EHR scenario: registering new patients in a clinic including assigning him the clinicians (doctors, nurses, etc.), reading and updating a record, retrieving patient information from external sources, and providing the results of examinations and treatment to authorized externals clinical entities.

The access to an EHR depends on several factors:

- The sensitivity type of the record.
- The type of patient, say if the patient is a celebrity (VIP)[1] or not, and on the patient having opted-in for a special more restrictive access control management of the EHR. Thus, if the patient is VIP or has opted for this restrictive policy, his default records will be of restricted type. If not, the default access control for the typical record is that all doctors of the practice or ward have access to it.

[1] In some countries the privacy of VIPs is specially protected, while in others this would be a very awkward assumption. Nevertheless, our choice is without any loss of generality: if there is no difference between patients we may simply assume all are VIPs (or none).

- The relation of the patient to the requester of the record (for instance, if the requester is the treating doctor or is in the same practice or clinic ward as the treating doctor).
- The consent that the patient has given.
- The access purpose, in particular, if the request is made in an emergency case.
- Regulation.

Ideally, access control policies should be written in such a way that the different policy conditions (EHR sensitivity types, clinician roles, local regulations, etc.) can be written independently from each other and composed when the system is initialized.

We can assume that most of the EHR for the patient is of type *normal-EHR*, but there may occur situations where this is not the case.

3 Access Control Rules

The precise rules describing the permissions of users to access EHRs that are assumed as follows:

- The treating doctor[2] may read or append to any record in the EHR.
- The patient may read or append to any of his records, except in the case he does not have the legal age for that purpose (determined by law) or in case of statutory exemptions (court decisions, etc.). The decision may indicate that a particular family member, the guardian or custodian, or the treating doctor himself play the role of the patient for the purposes of this policy and for the policies regarding user consent and notification. The existence of such a court decision (or legal exception), is marked in the *meta-data* of the EHR DataBase.
- Any clinician of the same ward or practice may read or append to records of type *emergency-EHR* or *normal-EHR*.
- Any clinician in same network or system may read *emergency-EHR* records.
- For any other doctor the following condition holds: If he is able to connect and strongly authenticate to the Network or System, he may read or append to any record if the patient (and in some systems if the treating doctor) has consented this action.
- In case of a referral, the referring doctor may read the records of the doctor who made the corresponding examination.

[2]For our purposes, each patient has one treating doctor. In more complex scenarios, each EHR is associated to exactly one treating doctor, but the patient may have different treating doctors (in different contextes).

Actions on the EHR are restricted further with the following obligations[3] and constraints:

- For each read and write action, a log must be written (for audit).
- Each write action can only append or attach comments, information, etc. Existing entries can not be deleted, before a certain time. They must be deleted after some other time.
- Each information appended must be time-stamped and signed at the moment of appending.

4 Initial Setting

For the sake of concreteness, we may assume initially the following scenario: there are two medical centers (North and South Hospitals) with a total of 3 Wards ("LeftWing" and "RightWing" in the North Hospital, "First Floor" in the other); each Ward has one Doctor. This is shown in Figure 1, which should be self-explaining. Note that there are two doctors, Carlos and Carol, that are not assigned to any of the wards above (they may be assigned to other institutions not shown in the figure).

Note: in the Figures we use a convention: The patients are assigned to doctors, who themselves are assigned to a Ward in a Medical Center. Thus the patients are assigned (in the Figures) *implicitly* to Wards. In reality (and later in a variation of this scenario will play a role, see Subsection 5.2) we need patients to be *explicitly* assigned to Wards (besides doctors).

5 Dynamic Scenario

Starting from the *initial situation* described above, we will now consider some variations. They can be summarized as follows:

- A nurse change from one ward or hospital to another.
- The association of a doctor to ward or hospital changes.
- A patient is being referred to a specialist.
- A doctor is in vacation and has a substitute.
- A patient moves to a different practice or hospital.
- A patient undergoes an emergency situation.

The different variations may happen in any order and combination.

[3]The obligations are considered to be independent of the permissions and of the mechanisms used to enforce the access control. This means that obligations must be fulfilled in any case of access, also in cases where the access control mechanisms were somehow bypassed (which should never happen, but sometimes does). That is, we want the obligations to be fulfilled, even under abnormal behavior.

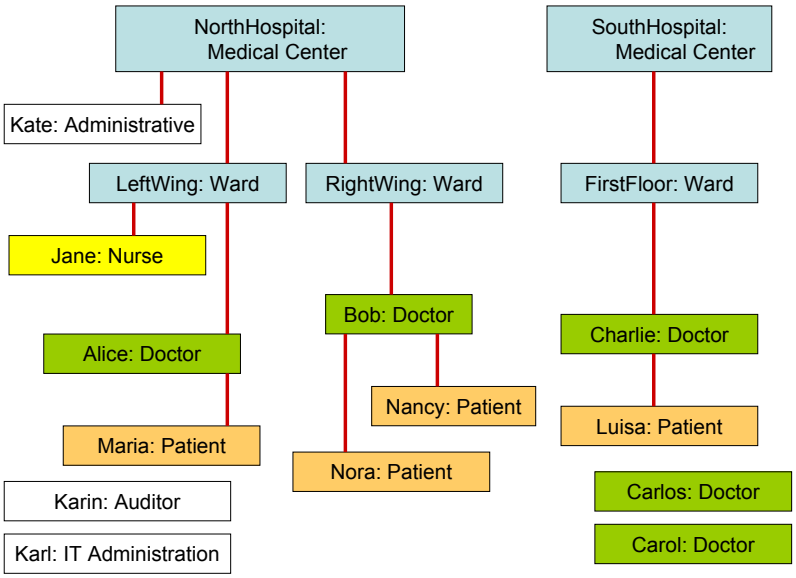

Figure 1: The initial Setting of our scenario

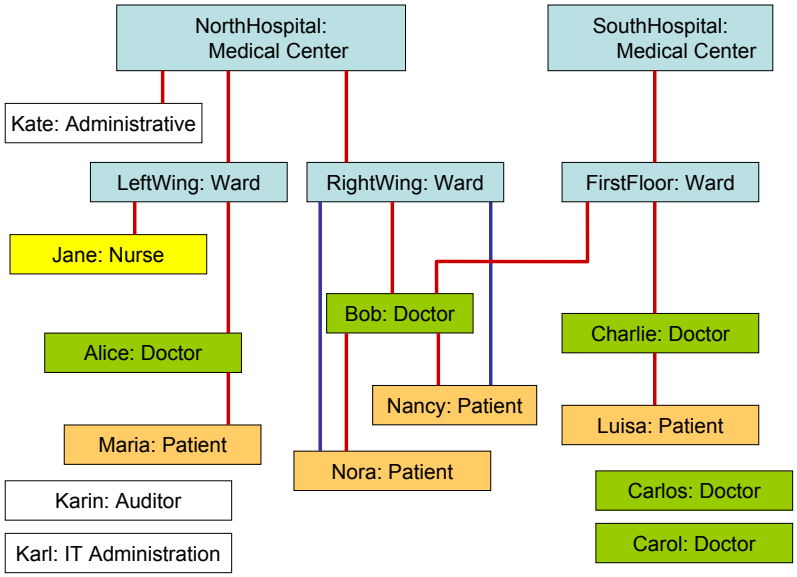

Figure 2: The Doctor Bob is associated to two Hospitals

5.1 The Association of a Nurse to Ward/Hospital changes

In our scenario we will assume that Jane moves from the Left Wing in the North Hospital to the First Floor of the South Hospital. When she does that, immediately her access rights to the EHRs of the patients (Maria and Luisa, in this case) change accordingly.

5.2 The Association of a Doctor to Ward/Hospital changes

We assume that a doctor can be assigned to two (or more) wards in one or several hospitals. In our scenario, Bob, from the Right Wing is assigned to a second ward, the first floor, in the other hospital. Note since Bob is associated to two wards, at least here it is necessary to explictly mention the association of the patients of Bob to wards (both Nancy and Nora are associated to the Right Wing).

When Bob is associated to the two wards, he may access patient information (in particular: normal EHRs) in both of them. Later, the assignment of Bob changes back to the original situation: the Right Wing.

5.3 The Patient is referred to another Doctor

Patients with particular symptoms may be referred for further evaluation, to specialized treatment, or a particular treatment or medicine.

In our scenario, Alice, the treating doctor of Maria, decides that she may benefit from further specialized health evaluations, which can be provided by another doctor, Carlos. For this purpose, Alice writes a *referral EHR*, describing the reason of the referral and the relevant aspects of the situation of the patient. The referral EHR is meant to be read by Carlos, but the patient has to *consent* that access.

5.4 A doctor is in vacation and has a substitute

A doctor, Bob, goes in vacation, and another one, Carol is his substitute. The patient, Nora, does not have to consent this change, but has to be *notified* that this is the case.

5.5 The Emergency Situation

Doctors are always allowed to access (read or append) an existing EHR in the case of emergency. Thus, any doctor may decide to access the EHR, by entering as special reason "emergency". The doctor that has entered the "emergency case" for the patinet can read or write any EHR of the patient for a (short) perioed of tme (say, an hour), after which he may decide to enter the "emergency case" case again, if needed. The access to the EHRs is protocolled precisely and the patient and auditors in the hospital are notified.

5.6 Access to the EHR Meta-Data

"Meta-Data" of the EHR DataBase is data related to electronic Health Records, but as such does not represent EHRs. It may be included in the same EHR DataBase but it can be a physically separated DB). Meta-data can include

- logs used for audit purposes,
- the associations between entities (doctors, nurses, hositals, wards, etc),
- the facts that notification has been provided to the patient or consent from the patient has been given, etc.
- the existence and implications of court decisions, etc. that affect the role of the patient.

The access to meta-data is very restricted, for obvious reasons. Logs must be written anytime a change to access control conditions happen or anytime an access to an EHR happens. They can not be deleted before a very long time (in the order of years) Audit logs can only be read by auditors, a special group of people that does not contain medical practitioners not patients of the system.

The associations between the entitites can only be modified by a selected group of "administrators".

The status of notifications or consent (or other events) is written exactly when those events happen, and can only be read by the system routines that verify the access control to EHRs. (This may be too restrictive though).

Court decisions and their implications can be written only by priviliged medical personell based on a four-eyes principle.

References

[1] R. J. Anderson. A Security Policy Model for Clinical Information Systems. In *1996 IEEE Symposium on Security and Privacy*, pages 30–42. IEEE Computer Society Press, 1996.

[2] A. C. Simpson, D. J. Power, M. A. Slaymaker, D. Russell, and M. Katzarova. On the development of secure service-oriented architectures to support medical research. *International Journal of Healthcare Information Systems and Informatics*, 2(2):75–89, 2007.

[3] J. Ure, J. Geddes, C. Mackay, S. Lloyd, A. Simpson, D. Power, D. Russell, M. Jirotka, M. Katzarova, M. Rossor, N. Fox, J. Fletcher, D. Hill, K. McLeish, Y. Chen, J. V. Hajnal, S. Lawrie, D. Job, A. McIntosh, J. Wardlaw, P. Sandercock, J. Palmer, D. Perry, R. Procter, M. Hartswood, R. Slack, A. Voss, K. Ho, P. Bath, W. Clarke, and G. Watson. Designing for e-health : Recurring scenarios in developing grid-based medical imaging systems. In *HealthGrid*, June 2006.