A Digital Rights Management Model for Healthcare

(Position Paper)

Nicholas Paul Sheppard
Department of Computer Science
University of Calgary
Calgary AB T2N 1N4, Canada
E-mail: nsheppar@ucalgary.ca

Reihaneh Safavi-Naini
Department of Computer Science
University of Calgary
Calgary AB T2N 1N4, Canada
E-mail: rei@ucalgary.ca

Mohammad Jafari
Department of Computer Science
University of Calgary
Calgary AB T2N 1N4, Canada
E-mail: jafarm@ucalgary.ca

Abstract—Electronic healthcare records promise to increase the efficiency and effectiveness of healthcare systems, but also introduce new risks to the security and privacy of healthcare information. In this paper, we outline how digital rights management can be used to protect health information transmitted throughout a distributed healthcare system. Our proposal allows for information to be disclosed on a need-to-know basis as defined by workflows, and in line with the wishes of patients.

I. INTRODUCTION

Electronic healthcare record systems promise to increase the efficiency and effectiveness of healthcare systems by ensuring that healthcare workers can get timely access to the correct and complete information that they require in order to provide good health services to their patients. Electronic healthcare systems have been investigated in many countries, and numerous research journals and conferences are devoted to their design and evaluation.

Distribution of information through an electronic healthcare system, however, carries a risk that patients’ information will be misused, resulting in invasions of privacy and/or unfair discrimination on the basis of patients’ medical histories. Security and privacy therefore forms an important part of any electronic healthcare system.

In particular, the principle of consent is widely used in privacy law to restrict the disclosure of sensitive information according to the wishes of the subject of that information. Electronic consent systems allow the subject of some electronic information to permit or deny the disclosure of that information to particular people in particular circumstances [1]. Electronic consent systems have been proposed as a method of controlling the disclosure of healthcare records [2]–[5], as well as other kinds of personal information [6], [7].

Electronic consent systems bear some resemblance to digital rights management systems (“DRMs”). Digital rights management is best known for its use in the protection of intellectual property [8], but can also be applied to the protection of personal information [9]. Digital rights management technology allows information owners to control the distribution and use of information by describing a policy in a machine-readable licence. Information is distributed in a protected form such that it can only be accessed by special DRM agents that are trusted to comply with licences.

Petković, et al. argue that digital rights management technologies already provide many of the features desired in a secure electronic healthcare system, in that they can provide persistent and homogeneous protection of information even when it is disseminated throughout a distributed healthcare system [10]. In this position paper, we describe a model for a secure electronic healthcare record system based on the digital rights management approach to privacy protection and workflow-based access control [11].

While many of the features of the proposed system could also be provided by an access control system and/or electronic consent system such as those proposed in earlier work, the proposed system additionally allows for

- persistent protection of information throughout the top-level electronic healthcare record system, local healthcare facilities and mobile devices; and
- automatic enforcement of patients’ consent objects.

We also introduce some new techniques with wider applications in digital rights management, including

- the use of workflow information to provide fine control over the purposes for which data is used; and
- the ability to transfer the execution of a task from one device to another (known as session mobility [12]) within a digital rights management system.

II. DIGITAL RIGHTS MANAGEMENT

Digital rights management can be defined as “persistent access control”, in that it controls access to data irrespective of its physical location [13]. Unlike traditional access control systems, digital rights management allows protected information to be transmitted over insecure channels and stored on insecure storage devices without compromising the integrity and confidentiality of the information.

Fig. 1 shows our reference model for a digital rights management system [8]. Information is created by a provider, and transmitted in a protected form to a user via some distribution channel. In order to access the protected data, the user must obtain a licence from the licence issuer.

Licences contain the terms of use of the data written in a machine-readable rights expression language, together with the secret information required to access the protected content. Licences thus play the role of the access control policy in traditional access control systems.
The secret part of a licence is packaged so that it can only be accessed by a special DRM agent, which is a tamper-resistant piece of software or hardware guaranteed by its manufacturer to behave in accordance with licences. The DRM agent effectively plays the role of the “reference monitor” in traditional access control systems.

III. A DRM MODEL FOR HEALTHCARE

The system proposed in this paper can be seen as a two-stage digital rights management system, composed of

- a “global” (in practice, national or regional) rights management system that controls the distribution of healthcare information to healthcare facilities; and
- a facility-level rights management system that controls the distribution of information within facilities.

Patients express their consent, and jurisdictions express their laws, in very broad terms at the global level. Individual facilities enforce the global policy by mapping the specific actions, actors, items of data and workflows used within the facility to their global counterparts.

A. Global Secure Healthcare Record System

Fig. 2 shows an overview of the secure electronic healthcare record system proposed in this paper. It consists of

- an arbitrary number of patients;
- an arbitrary number of healthcare facilities in which patients may seek treatment;
- a consent management system (“CMS”) that stores patients’ consent objects, which record patients’ consent (or not) to use information about them; and
- a healthcare record database (“HRDB”), in which patient records are stored.

Both the consent management system and healthcare record database are logically centralised, though in practice they may in fact be composed of an arbitrary number of physically distributed databases.

We can think of the system shown in Fig. 2 as being a digital rights management system in which healthcare workers are the providers, the consent management system is the licence issuer, the healthcare record database is the distributor, and healthcare facilities are users, with “DRM agents” implemented by the facilities’ digital rights management systems.

Consent objects are created by patients themselves, but are stored in the consent management system. Consent objects must be requested by individual healthcare facilities whenever someone in that facility requests to access a patient record to which that consent object applies.

Healthcare records are created and modified by individual workers within the facilities that are involved in the treatment of the patient to whom the records refer. Any new or modified records must be transmitted to the healthcare record database, from where they may be requested by other workers.

B. Healthcare Facilities

We propose that all of the sensitive activity within a facility be controlled by workflows designed and maintained by that facility. Workflows set out the steps that must be undertaken in order to accomplish a given complex task. Our system uses workflows both to identify which people require which rights in order to carry out their work, and to map an access control request to a broader purpose to which it contributes. Workflow design is a significant issue on its own (see, e.g., [14]), but we believe that our model can support any workflow.

Fig. 3 shows an overview of a single healthcare facility with a workflow in progress. Every healthcare facility contains

- a policy officer who designs workflows, assigns users to roles, and designs the facility’s access control policy;
- a workflow management system that controls all of the workflows in the organisation;
- an identity management system that verifies credentials for individual workers within the facility, and assigns individual workers to roles within the facility;
- a licence issuer that translates consent objects and workflow information into licences;
- a record packager that translates patient records into protected documents; and
- a session controller that controls the admission of DRM agents to sessions (defined below).

All of the information flow within a healthcare facility is controlled by a digital rights management system. All information retrieved from the global electronic healthcare system must be transformed into rights-managed information according to this system, and workers within the facility must perform all tasks that relate to electronic patient records using DRM agents that conform to that system.

Every step of a workflow described in the workflow management system is associated with one or more authorisation templates that describe the (minimum) rights required to
perform the actions required by that step [11]. An authorisation template takes the form of a licence for carrying out the corresponding step, but leaves “holes” for the receiver of the licence, and the items of data used by the licence. These must be filled in at instantiation-time with the particular actor and data involved in the instantiated workflow.

All actions that require access to sensitive information are undertaken within the context of a session. A session is an abstract entity with the same basic architecture as the authorised domains widely used in modern digital rights management systems [15]. Licences may be issued to a session, and DRM agents may become members of a session by applying to the session controller. Any DRM agent that is a member of a session may use licences issued to that session. In our proposal, a session is created for every workflow instantiated by the workflow management system. All of the licences necessary to complete the workflow are issued to the session, and the worker assigned to that workflow may log in and out of the session using any suitable DRM agent.

A licence may contain a constraint indicating that it is only valid while the workflow is executing the step for which the licence was created. A DRM agent can check this constraint by contacting the workflow management system. Once the workflow progresses beyond this step, users may not perform the action permitted by the licence.

C. Policy Expression

Our proposal allows consent objects and authorisation templates to describe policies that refer to users and roles; healthcare records and categories of information; and purpose of use. Such policies can be enforced using information from the identity management system; healthcare record database; and workflow management system, respectively.

Consent objects, authorisation templates and licences can be expressed in a language such as the Open Digital Rights Language [16], as in Fig. 4. This consent object gives consent for members of Facility 1 to read (“play”) a patient’s record for the purpose of a diagnosis workflow. Such languages may be extended to contain rights and constraints used in healthcare.

Upon receiving a request to instantiate a workflow, the licence issuer of a facility is responsible for transforming the authorisation templates for the proposed workflow into requests for the consent management system. In doing so, it translates any local identifiers for users, roles, items of data, and purposes into equivalent global identifiers and transmits these to the consent management system. The consent management system is then able to compare the proposed licences with the relevant consent objects and return a response.

D. Emergency Over-Ride

In an emergency situation, suitably authorised workers may apply to over-ride a workflow or a consent object. In this case, the licence issuer may issue licences to access data even if the policy officer or patient has not explicitly given consent for such licences to be issued. We expect that such licences would be associated with an expiry time, and that any requests to issue them would be logged for later review.

IV. WALK-THROUGH

Suppose that a patient arrives at a healthcare facility with a complaint. We suppose that the facility has some workflow defined for diagnosing this kind of complaint. This workflow is to be instantiated in order to handle the new patient.

The first step is to assign a worker to perform the diagnosis, and to identify the resources that will be acted upon by the workflow. We will refer to the worker as the subject of the workflow. The authorisation templates of the workflow may specify a role that this worker must belong to, which can be checked by conferring with the identity management system.

The second step is to propose a licence for each step of the workflow by filling the “holes” of the corresponding authorisation template with the subject and resources identified in the first step.

The third step is to check that the proposed licences are consistent with the patient’s consent object. The licence issuer transforms each proposed licence into a request for the consent management system. The system may refuse permission to issue one or more of the licences, or it may request that they be modified. If the proposed licences cannot be made consistent with the relevant consent objects, the licences must not be issued and the workflow must not be initiated.
If the proposed licences are acceptable, however, the workflow management system may instantiate the workflow and create a new session to act on behalf of its subject. The licence issuer may then issue the licences to the new session.

The human subject of the workflow may then log-in to one or more DRM agents using credentials that can be verified by the identity management system. Once a DRM agent has been logged into, it can request to join the new session. If the user logs out, it must leave the session.

The record packager must then retrieve the patient records to be used by the new workflow instance from the global healthcare record database, and transform these into the format used by the digital rights management system. In this form, they can be transmitted to the DRM agents used in the session.

When the human user instructs a DRM agent to perform some operation on a protected record, the DRM agent must check that a valid licence exists for performing this action. If not, the instruction must be refused. Otherwise, it may use cryptographic information in the licence to decrypt the record and perform the requested action.

V. SECURITY

Our proposal aims to permit access to personal health information only if the access is required by accepted medical practice, and only if the patient to whom the information refers has granted (or, in an implicit-consent regime, not denied) consent for his or her information to be accessed. Our proposal can furthermore assure the integrity of health information.

In our proposal, the policy officer of a facility acts as the source of accepted medical practice by providing the workflows, authorisation templates, and user-role mappings that describe this practice and the authorisation policy that it implies. The consent management system acts as the source of patient consent.

The foregoing policy will be enforced if:

- the licence issuer only issues licences that are derived from the authorisation templates of legitimate workflows;
- the consent management system only approves requests to issue licences if they are consistent with the relevant consent objects;
- the session controller only admits a DRM agent into a session if its current human user has been assigned to the workflow instance that that session represents; and
- the record packager translates health information into a form in which it can only be accessed by the digital rights management system, and cannot be tampered with.

It should be noted, however, that the security of the system depends to some degree on the trustworthiness and reliability of both its administrators and users. It cannot coerce policy officers into creating good policies, and has only limited ability to coerce good behaviour from users. In particular, our system cannot prevent a number of physical attacks (or accidents) made by insiders, including:

- attacks in which an unauthorised person obtains access to a device that has been authenticated as being operated by an authorised person;
- attacks in which an authorised person records information in an analogue form after being granted access to it; and
- attacks in which a privileged person does not behave in accordance with the requirements we have set out above.

VI. CONCLUSION

Digital rights management can be combined with ideas from electronic consent and workflow-based access control to enforce security policies that combine the needs of healthcare practitioners with the desires of patients. Digital rights management extends traditional access control systems with protection that persists throughout centralised databases, individual healthcare facilities, and other organisations that have a need to access healthcare information.

REFERENCES