Securing Medical Research Data with a Rights Management System

Mohammad Jafari[*], Reihaneh Safavi-Naini[*], Chad Saunders[**], and Nicholas Paul Sheppard[***]

[*]Department of Computer Science, University of Calgary
[**]Department of Community Health Science, University of Calgary
[***]Library eServices, Queensland University of Technology

Abstract

We propose a digital rights management approach for sharing electronic health records for research purposes and argue advantages of the approach. We give an outline of our implementation, discuss challenges that we faced and future directions.

1 Introduction

There is increasing pressure on healthcare researchers to bridge the gap between bench-based basic science research and actual use within medical practice. This translational research, commonly referred to as *bench-to-bedside*, requires a very different approach compared to traditional methods [4]. In particular, translational research often requires integrating data from multiple systems and of different types. Some of this data is collected as part of the ongoing care of these patients and re-purposed for re- search while some of the data is collected specifically for individual studies. Guiding the use of this data for translational research is the ethics review process that attempts to ensure that patients provide their informed consent for the use of their data for specific research purposes.

While this is reasonably easy to manage within the context of traditional health research methods since these tend to be self-contained research projects that collect all the data required as part of the study, translational research tends to require re-purposing data, which further complicates the ethics review process. In addition, some of the most innovative translational research emerges from linking data collected for one study and domain, to data from another study in a separate domain.

Supporting this linking of data and the subsequent collaboration necessitates a system that ensures that ethics consents are enforced across studies and individual researchers, while facilitating the secure sharing of data and its movement among systems for the purposes of reporting and analysis, all in accordance with the consent.

De-identification of data for making it available within a collaborative environment is one very active area of research [3]. However, it is mainly aimed at making data available to public and either removes identifiable information, or perturbs sensitive values. Both of these methods reduce reliability and traceability of data and make it unacceptable in many research projects.

In this paper, we describe an approach to monitoring and enforcing ethics consents based on *digital rights management* ("DRM"). DRM provides "persistent access control" by which access to electronic data can be governed by a policy expressed in a machine-readable *licence*, regardless of the location in which the data is stored or used [2]. In the present context, the rights-managed data is a patient's electronic healthcare record ("EHR") and licences are derived from the patient's consent to use this record in a research context.

2 Our Work

We designed a DRM solution around a knowledge-base for the Hepatology Research Group at the Faculty of Medicine, University of Calgary, Canada. The main privacy requirements of the research facility are:

- researchers can only access the EHR of the project they are assigned to;
- the EHR can only be assigned to a project if the patient has consented to participate in that project;
- users can access project data based on their role in the organization and the project;
- the user can only exercise the specified access rights (e.g. read); and
- the access control will be persistent, in the sense that data remains protected on both server and client side.

We chose Microsoft's Active Directory Rights Management Services ("AD-RMS") [1] as the basis of our rights management solution, since the Hepatology Knowledge Base is based on Microsoft's SharePoint platform and this platform provides some support for AD-RMS. Users' identity information is stored and managed by Microsoft Active Directory, and access to rights-managed data is controlled by an AD-RMS-enabled version of Microsoft Excel.

Figure 1 shows an overview of our system. EHRs and consents are stored in a backend database and records are

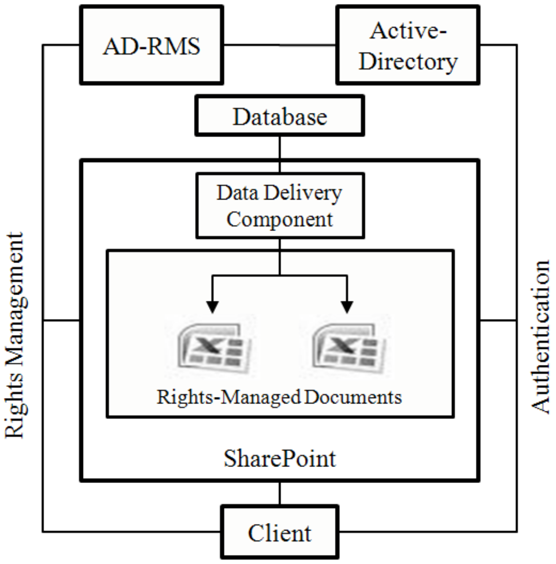

Figure 1: Securing the Hepatology Knowledge Base with AD-RMS.

assigned to projects through a selection process that we do not discuss here. Patients' consent comes in a simple form as a list of research projects for which he or she has consented to participate. For each project, a number of reports is designed that provide different types of reporting on the EHRs of the patients enrolled in that project.

SharePoint provides a rich environment to define and support role-based access control and the permissions on each view can be set so that only project members with certain roles can access them.

SharePoint can be integrated with the AD-RMS server, and provide persistent access control so that server-side permissions can be enforced on the client-side as well. For instance, if a user is not allowed to modify a document based on the permission settings on the server, he or she cannot modify that document even after the document is downloaded from the server and stored on the local machine. Neither is the user able to save a copy of the document and modify that copy.

Since SharePoint-RMS integration only supports protection of Microsoft Office documents, and since the EHR data is stored in a relational database the existing SharePoint integration could not readily be used for protection of EHR data. Hence, we implemented a data delivery component (depicted in Figure 1) as a SharePoint application that fetch the data from the database and store it in a Microsoft Excel document. Using this component each report comes in the form of an Excel document that is filled with fresh data whenever the user opens it.

A user can see all the reports to which he or she has some access by pointing his or her browser to the URL of the application website. The user can choose and download the latest version of the report to her machine. This is a protected copy that is encrypted and requires a license. To open the document, the user logs on the AD-RMS server, using Microsoft Excel. After logging in, the credentials of the user is checked and if they are eligible, a suitable licence is generated and sent to the agent with which the document can be decrypted. Excel will enforce the usage policy of the document.

3 Concluding Remarks

Using licences to express the access policy allows a fine-grain specification of access rules. It also allows an automated way of enforcing patients' consent. This approach can be used as an alternative or complementary approach to de-identification.

Although combining and reconciling patient consents with organizational policies has not been a major issue in the current system, in future extensions it might be. In the current system patient consents are enforced by defining project-specific views to the database in which the consents are taken into account. The organizational policy on the other hand, is defined and enforced using access control features of SharePoint. However, if patient consents take more complex forms in a way that they cannot be easily incorporated in definition of database views, defining, combining, and enforcing these two sets of independent policies will be an issue.

Although our decision for using spreadsheets was in the first place due to limitations in SharePoint's support for rights management, this approach also fits researchers' needs for doing various analyses and nicely matches certain use cases in practice, such as collaborations within a research team.

The digital rights management approach is scalable and although we only considered a single organization, one can extend the approach to multiple organizations.

References

[1] Microsft Active Directory Rights Management Service. `http://technet.microsoft.com/en-ca/windowsserver/dd448611.aspx`.

[2] Q. Liu, R. Safavi-Naini, and N. P. Sheppard. Digital rights management for content distribution. In *ACSW Frontiers '03*, pages 49–58, 2003.

[3] L. Sweeney. /k/-anonymity: a model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, 10(5):557–570, 2002.

[4] S. H. Woolf. The meaning of translational research and why it matters. *The J. of American Medical Association*, 2008.