Usage Management of Electronic Medical Records

Christopher C. Lamb, Pramod A. Jamkhedkar, Gregory L. Heileman, Ravi Kadaboina
University of New Mexico
Department of Electrical and Computer Engineering
Albuquerque, NM 87131-0001
{*cclamb, pramod54, heileman, ravik*}*@ece.unm.edu*

***Abstract*—Electronic medical record management is under new scruitiny as private companies move into the market and government agencies actively address percieved health care distribution inequalities and inefficiencies. Current systems are coarse-grained and provide consumers very little actual control over their data. Herein, we propose an alternative system for managing the use of healthcare infomormation. This system is more granular, allows for data mining and repackaging, and gives users more control over data while allowing said data to be distributed as much as needed. In this paper, we outline the characteristics of such a system, present relavant background information and research leading to the system design, and cover two specific use scenarios supported by this system that are difficult to control using simpler access control strategies.**

***Keywords*-usage management; electronic medical records**

I. Introduction

New healthcare legislation has spurred previously unknown levels of public and private investment into technologies supporting more efficient healthcare delivery [12]. An active area of examination is electronic health records. Current systems, like Microsoft HealthVault and Google Health are a start in this area, but provide rudimentary control over health information, provide consumers with very little actual control of their information, and essentially demand proprietary lockin to these products because of the amount of effort involved with data transfer [24].

We propose an open, consumer-centric approach to health information storage and consumption centered around flexible and granular usage management policies. User empowering systems in this area are needed to allow users control over the information that represents them, and would be in high demand if appropriately designed [9]. We propose to address this need by bundling health information (either entire records or subsets of records) with traceable and aggregateable usage policies controlled by the users themselves. Users would have the ability to make aspects of their records available to everyone from research institutions looking for historical information for studies, to specific healthcare providers who need specific information to support diagnoses. Furthermore, institutions would be able to combine information from groups of users and determine dynamically via policy evaluation how that new set of data can be used in a way that complies with all included user policies. If the combined dataset cannot be used, policies can be analyzed to determine the cause of the policy conflict.

We will propose, design, and demonstrate a system that supports granular management of the data elements of an electronic medical record. This management will allow users to specify policies over the data itself rather than the entire record in question, providing control over information dissemination. We will demonstrate this control in three distinct scenarios. The first will include two distinct parties negotiating over access to specific information contained in a medical record. If the parties can reach an agreement, the information consumer will be granted access to specific medical data, for an agreed-upon price. The second demostrates a data broker combining a set of previously acquired medical record data into an aggregate set for research, if the licensure is in fact compliant between all selelected data elements. Finally, the aggregated data set will be placed back into the market.

This kind of system, allowing users control over their data in ways fostering ease of dissemination, use and reuse, helps users receive better, more targed care, helps providers easly access required information, and allows this kind of data to be more easily examined and mined. We use established system design principles, used in the develoment of internet-scale networks to create a open flexible system [5], [8], [11]. We will standardize certain features, such as operational semantics and ontological domains, but otherwise limit the impact of the policy system on data dissemination as much as possible.

A. Previous Work

Past research applicable to this area includes usage management, digital rights management (DRM), and access control. Most of the research applicable to the combination of previous arfifacts into a single aggregate artifact comes from the DRM world in particular. Generally, these expressive languages have been fundamentally based on different types of mathematical logic or formalisms with reasoning capabilities [6], [7], [10], [13], [14], [21], [26]. This approach, while useful in closed systems, tends to not work as usefully in more open dynamic environments. This has led to the development of translation mechanisms to address interoperability needs [15], [20], [23]. This translation

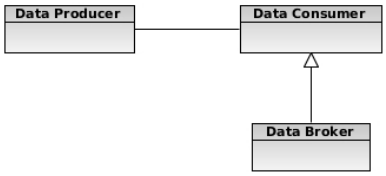

Figure 1. System Roles

process is difficult for most policy languages, and in fact infeasible as a result [19], [22]. Alternative approaches have required the use of sophiticated and powerful languages that must be adopted as a universal standard [1], [2], [25], [27]. This approach inherently limits innovation and flexibility [15], [16], [17], [18].

II. Underpinnings

The system we describe in the following sections incorporates a market to allow users and brokers to profit from the use of electronic medical data released under mutually acceptable terms, where usage policies accompany filtered data for either dynamic or static evaluation. Usage policies themselves are essentially unlimited in how they describe the use of a specific medical record.

A. Marketplace

Here, we incentivize electronic medical record adoption via the use of a data marketplace. We have three primary categories of users in mind:

- *Data Producers* who produce and market electronic medical information. This category is generally limited expressly to individual users who require medical care and other related products.
- *Data Consumers* who directly consume medical information. This category includes physicians, research institutions, and the like.
- *Data Brokers* who acquire and remarket medical data from data producers, making that data available in some kind of value-added for to data consumers. They are a proper subset of data consumers.

Data Producers would use the medical data market to profit from their personal information. When negotiating over specifics concerning how their data can be used, they are free to manipulate any aspect of the usage terms prior to a final agreement with a *data consumer*. The *data consumer* can accept or reject a specific proposal, as can a *data producer*. A typical negotiation would look something like this:

1) A *data consumer* searches the marketplace for medical information meeting specific requirements. This step is a call to a specific search interface in our example, but could be a manual process.
2) The search yields some results. This proposed system returns a list of contact information of known *data producers* that have data matching the search requirements.
3) The *data consumer* initiates a negotiation for access to specific data.
   a) The *data consumer* contacts the *data producer* and submits and initial proposal.
   b) The *data producer* responds to the initial proposal, either be indicating acceptance, rejecting the proposal, or submitting a counter proposal.
   c) The *data consumer* is then free to respond with acceptance, rejection, or a counterproposal of her own.
4) Eventually, the negotiation will conclude with the parties having reached an agreement describing access to specific medical data with associated term or having failed to come to mutually acceptable terms with respect to data access.

Usage terms in a successful conclusion generally describe what the *data consumer* can access, how and for how long, where it may be accessed, and so on. It will also usually describe some kind of payment for use, which can be based on any arbitrary number of factors such as time, date, location, attribution, or perhaps in combination with other data.

The market implemented in this system is built around JADE, an open source agent develoment framework based on FIPA agent specifications [3], [4].

B. Usage Management

describe how the usage management system works

C. System Ontology

This system is built around a common ontology that needs must be understood by any system developers. It is currently used to define relationships and entities within the system at design and run time. The primary elements in this ontology are:

- *Producer* This is a data producer as defined in our user model. A data producer owns a given *record* that has been created over a lifetime of medical care.
- *Consumer* Again from the user model, a data consumer. Data consumers use medical data in some way.
- *Record* A medical record. We can envision this as a set of discrete medical facts.
- *Filter* A transformation of a medical record. If we have a record r, we can transform r into r' by applying a transformation t such that $r' = t(r)$ where $t : record \rightarrow record$ and $r' \subseteq r$.
- *Filtered Record* A filtered record is a record to which a filter has been applied. If we have a filtered record r' derived from a record r, then $r' \subseteq r$.
- *License* A license describes the usage policy associated with a given filtered record. This controls all aspects

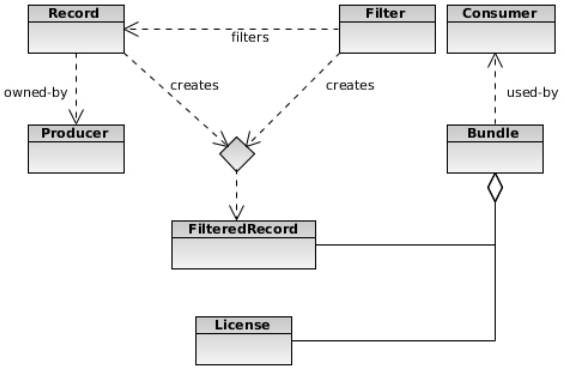

Figure 2. System Ontology

of filtered record use by an associated consumer. The specific terms are negotiated over by the producer and the consumer until some consensus is reached, and they then bind the use of an associated filtered record. Licenses must provide the ability to trace use of transitively associated artifacts regardless of the degree of separation as well. For example, if we have an artifact a composed of sets of data elements $e_0, e_1, ..., e_n$ derived from records $r_0, r_1, ..., r_n$, we need to be able to ensure that any use of a set of data elements $e_i, i < n$ is within the policy bounds of record $r_i, i < n$ and any compensation associated with such use is correctly attributed to the original data owners and brokers.

- *Bundle* A filtered record and associated license. This is distributed to data consumers.

D. Dynamic and Static Policy Evaluation

define dynamic and static policy evaluation, elucidate specific advantages/disadvantages of each, go over which we need to use here and why

III. System

A. Cases and Scenarios

Outline the use cases, describe them, map them to specific scenarios

B. Scenario 1: Negotiation

Demonstrate and present results; negotiation over specific information contained in a EMR

C. Scenario 2: Aggregate Assembly

Demonstrate and present results; assemble data elements into a single data set; show both usage term compliance and non-compliance

D. Scenario 3: Aggregate Submission

Demonstrate and present results; insert new set into marketplace; demonstrate acquisition of set and traceability back to individual elements

IV. Conclusion

Evaluate results and outline future work

Acknowledgment

The authors would like to thank ECE, Ravi, Greg, Pramod?

References

[1] Enabler release definition for DRM V2.0. Technical report, Open Mobile Alliance, 2003. xml.coverpages.org/OMA-ERELD_DRM-V2_0_0-20040401-D.p

[2] Open digital rights language ODRL version 2 requirements. ODRL, Feb. 2005. odrl.net/2.0/v2req.html.

[3] Java Agent DEvelopment Framework. http://jade.tilab.com/, January 2011.

[4] The Foundation for Intelligent Physical Agents. http://www.fipa.org, January 2011.

[5] Harald Alverstrand. The role of the standards process in shaping the internet. *Proceeding of the IEEE*, 92(9):1371–1374, 2004.

[6] Alapan Arnab and Andrew Hutchison. Persistent access control: A formal model for drm. In *DRM '07: Proceedings of the 2007 ACM workshop on Digital Rights Management*, pages 41–53, New York, NY, USA, 2007. ACM.

[7] Adam Barth and John C. Mitchell. Managing digital rights using linear logic. In *LICS '06: Proceedings of the 21st Annual IEEE Symposium on Logic in Computer Science*, pages 127–136, Washington, DC, USA, 2006. IEEE Computer Society.

[8] Marjory S. Blumenthal and David D. Clark. Rethinking the design of the Internet: The end-to-end arguments vs. the brave new world. *ACM Transactions on Internet Technology*, 1(1):70–109, Aug. 2001.

[9] Pyper C., J. Amery, M. Watson, and C. Crook. Access to electronic health records in primary care-a survey of patients' views. *Medical Science Monitor*, 10(11), 2004.

[10] Cheun Ngen Chong, Ricardo Corin, Sandro Etalle, Pieter Hartel, Willem Jonker, and Yee Wei Law. LicenseScript: A novel digital rights language and its semantics. In *Third International Conference on the Web Delivery of Music*, pages 122–129, Los Alamitos, CA, Sept. 2003.

[11] David D. Clark, John Wroclawski, Karen R. Sollins, and Robert Braden. Tussle in cyberspace: Defining tomorrow's internet. In *SIGCOMM*, pages 347–356, Pittsburg, Pennsylvania, USA, Aug. 2002.

[12] Federal Government of the United States of America. Tracking the money. http://www.recovery.gov, December 2010.

[13] Joseph Y. Halpern and Vicky Weissman. A formal foundation for XrML licenses. In *Proceedings of the 17th IEEE Computer Security Foundations Workshop*, pages 251–265, Asilomar, CA, June 2004.

[14] Joseph Y. Halpern and Vicky Weissman. A formal foundation for XrML. *J. ACM*, 55(1):1–42, 2008.

[15] Gregory L. Heileman and Pramod A. Jamkhedkar. DRM interoperability analysis from the perspective of a layered framework. In *Proceedings of the Fifth ACM Workshop on Digital Rights Management*, pages 17–26, Alexandria, VA, Nov. 2005.

[16] Pramod A. Jamkhedkar and Gregory L. Heileman. DRM as a layered system. In *Proceedings of the Fourth ACM Workshop on Digital Rights Management*, pages 11–21, Washington, DC, Oct. 2004.

[17] Pramod A. Jamkhedkar and Gregory L. Heileman. *Handbook of Research on Secure Multimedia Distribution*, chapter Rights Expression Languages. IGI Publishing, 2008.

[18] Pramod A. Jamkhedkar, Gregory L. Heileman, and Ivan Martinez-Ortiz. The problem with rights expression languages. In *Proceedings of the Sixth ACM Workshop on Digital Rights Management*, pages 59–67, Alexandria, VA, Nov. 2006.

[19] Rob H. Koenen, Jack Lacy, Michael MacKay, and Steve Mitchell. The long march to interoperable digital rights management. *Proceedings of the IEEE*, 92(6):883–897, 2004.

[20] Josep Polo, Jose Prados, and Jaime Delgado. Interoperability between ODRL and MPEG-21 REL. In *Proceedings of the first international ODRL workshop*, Vienna, Austria, Apr. 2004.

[21] Riccardo Pucella and Vicky Weissman. A logic for reasoning about digital rights. In *Proceedings of the 15th IEEE Computer Security Foundations Workshop*, pages 282–294, Nova Scotia, Canada, June 2002.

[22] Reihaneh Safavi-Naini, Nicholas Paul Sheppard, and Takeyuki Uehara. Import/export in digital rights management. In *Proceedings of the Fourth ACM Workshop on Digital Rights Management*, pages 99–110, Washington, DC, Oct. 2004.

[23] Andreas U. Schmidt, Omid Tafreschi, and Ruben Wolf. Interoperability challenges for DRM systems. In *IFIP/GI Workshop on Virtual Goods*, Ilmenau, Germany, 2004. `http://virtualgoods.tu-ilmenau.de/2004/program.html`.

[24] A. Sunyaev, A. Kaletsch, and H. Krcmar. Comparative evaluation of google health api vs. microsoft healthvault api. In *Proceedings of the Third International Conference on Health Informatics*, HealthInf 2010, pages 195–201, Setubal, Portugal, 2010. INSTICC.

[25] Xin Wang. MPEG-21 rights expression language: Enabling interoperable digital rights management. *IEEE Multimedia*, 11(4):84–87, October/December 2004.

[26] Jianwen Xiang, Dines Bjorner, and Kokichi Futatsugi. Formal digital license language with OTS/CafeOBJ method. In *Proceedings of the sixth ACS/IEEE International Conference on Computer Systems and Applications*, Doha, Qatar, Apr. 2008.

[27] eXtensible Rights Markup Language (XrML) 2.0 Specification, November 2001. `www.xrml.org`.