Usage Management of Personal 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 finer grained, 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 usage 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 in technologies supporting more efficient healthcare delivery [13]. An active area of examination is electronic health records. Current systems, such as 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 [29].

We propose an open, consumer-centric approach to health information storage and consumption centered around flexible and fine grained 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 [10]. 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 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 [6], [9], [12]. We 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 [7], [8], [11], [14], [15], [26], [31]. 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 [16], [22], [28]. This translation

process is difficult for most policy languages, and in fact infeasible as a result [20], [27]. Alternative approaches have required the use of sophiticated and powerful languages that must be adopted as a universal standard [1], [2], [30], [32]. This approach inherently limits innovation and flexibility [16], [17], [18], [19].

II. New Models

Engineers and futurists have speculated as to the impact of personal medical records for years [23], [24]. Others have speculated on the institutional use of personal medical records by organizations in today's regulated medical environment [3]. Health records, when under the control of the person they address, are no longer controlled by the Health Insurance Portability and Accountability Act (HIPPA), though the companies that manage them on the user's behalf in these cases are regulated in most aspects by the Electronic Communications Privacy Act [21]. In total, These concerns imply certain requirements on robust medical record systems, making use models and record control more complex. None of the promises or concerns of personal medical records can be realized or mitigated without strong usage management. With a dependable usage management capability, personal medical records open new horizons in the services landscape for interested adopters.

A. A Note on Reliability

In order for PMRs to be effective, they must be actively used by health care providers. A system with the wrong kinds of editability constraints or auditing capabilities is at risk of remaining unused by an individual's care providers. Ideally, these kinds of health records would contain the kind of information a physician would include in a patient's chart. This is information providers are required to maintain for adequate patient treatment. If this information can be arbitrarily edited however, it loses it's credibility.

In fact, many employer-sponsored monitoring programs may incentivize gold-plating medical histories. Systems like Virgin HealthMiles are marketing themselves directly to employers as ways to monitor employee health. [25]. Companies are using Virgin HealthMiles to track employee exercise, and as an incentive to use the product (and get more exercise), are offering additional contributions to employer-sponsored health savings accounts if employees meet certain criteria. Similar senarios could be right around the corner for personal health management systems, were employers incentivize employees to decrease blood pressure, change diet, or similar kinds of things. In those situations, the pressure for users to alter their records to reflect the reality their employers want to see will be immense, and many users are likely to resort to embellishing their records as a result.

Once that happens, health care providers can no longer use the records to provide care.

Any system managing these kinds of records must therefore provide mechanisms to certify, if not the accuracy of the provided information, at least the veracity of it. Care providers must be able to trust the information provided in a given record, and must not be required to shoulder the burden of viewing the record's edit history in order to do so. This implies a separation of roles between those who can edit the content of a given record, and those who control how the content of that record may be used.

B. Remote Information Access

Remote access to a patient's health care information is a standard feature of everyday life to which most of us pay little attention. While in school, we are required to provide evidence of vaccination. When older, travel to most parts of the world requires rounds of injections. Most travellers are strongly advised to purchase additional travel insurance to ensure appropriate care in emergencies. Certainly, when travelling to some parts of the world internet access can be difficult to acquire, but nevertheless such access is much more common now than it was event two years ago, and is becoming easier and easier to find with the proliferation of cellular telephone networks in hertofore undeveloped countries.

Open access to this kind of healhcare information would certainly make these scenarios easier to deal with for any user, but require strong usage management protections to be effective. In each case we have distinct sets of users that require access to care information, and in each case those users require access to a specific and limited sections of a personal healthcare record. School adminstrators, for example, need to confirm the vaccination status of students. This requires unfettered access to a student's vaccination history, but not to that student's psychiatric care or genetic record. Likewise, travel visa providers may need access to similar information. On the other hand, care providers no matter the country of origin require comprehensive care record access in order to provide timely and accurate care. Furthermore, users have different requirements with respect to the speed of access. School adminstrators have much less of an urgent, pressing need for care information that an Ethiopian doctor treating an injured patient.

Importantly, access need not be granted permanently. Both administrators and foriegn care providers could be given general role-based access that can be removed when no longer neccessary.

The ability to provide care information in a secure, manageable way in these scenarios saves users significant time and headache. Rounding up and delivering vaccination records to school adminstrators is time consuming and stressful. Receiving emergency health care in foriegn countries is more than a little frightening. Systems that can help ameliorate these kinds of situations would certainly be useful. Furthermore, without specific controls over specific

data elements composing a given record, these users cannot be appropriately limited in their access.

C. Monitoring

To constrain health care costs, some employers are beginning to implement holistic preventative health programs. These programs are structured to attempt to lower overall healthcare costs for a large group of employees through regular screenings, exercise programs, and key health marker monitoring. Employers are interested in monitoring indicators like trigyceride levels, serum cholesterol, HDL/LDL ratios, blood glucose, blood pressure, and the like. Employee participation is not neccessarily mandated, but can be encouraged through additional contributions to health savings accounts for participating employees. In these cases, employers have specific things in which they have an interest. Employees on the other hand likely have information in their care records they very much want to keep out of their employers hands. For example, an employee may very much want the additional HSA contribution for her family, but is not inclined to let her employer know about her antidepression medications or her recent treatment for alcohol dependency.

A dependable usage management system supports this kind of partitioned use. With appropriate controls, this information can be centralized and controlled by the record owner, who can create limited access for employers. Furthermore, this kind of information can be aggregated by the user over a period of years, demonstrating a pattern of healthy behavior, and perhaps making that record owner more attractive to future employers. Sensitive information can still be controlled by limiting access.

D. Custom Care

E. Data Marketplace

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.

III. Sample System - Data 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.

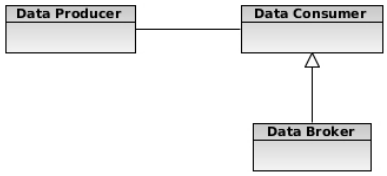

Figure 1. System Roles

- *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 they may use it 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 [4], [5].

A. 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 of filtered record use by an associated consumer. The specific terms are negotiated over by the producer and the consumer until some optimal 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.

B. Dynamic and Static Policy Evaluation

Usage policies can be evaluated over a spectrum bordered by two distinct approaches - either dynamically, at request time, or statically, when a bundle is created. Pure dynamic policy evaluation evaluates the entire policy against an artifact at *request time*, specifically and only when a request for an action is made by a consumer. Static evaluation only occurs when *the bundle is created* and is not evaluated at any later time. While dynamic policies are more powerful, static policies are generally simpler to define, create, and apply. Dynamic policy evaluation requires significant runtime infrastructure as well, which static evaluation will never require. Furthermore, that runtime infrastructure must be present in a variety of systems, implemented upon a myrad of platforms in a slew of different programming languages. Still, we have compelling reasons for developing dynamic evaluation systems. Static systems cannot evaluate dynamic properties well. Attributes like time are impossible to adjudicate with the simplest of static licenses and require some kind of dynamic evaluation. Likewise, evaluation of a bundle's context is equally impossible to do with simple static policies. Dynamic policies are more suitable for content that producers are interested in providing for unexpected use, while static policies generally only support predefined use scenarios.

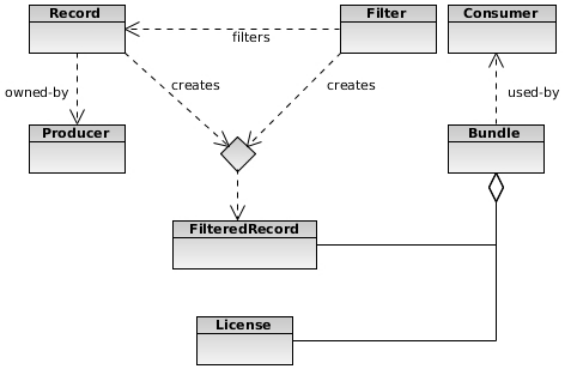

Figure 2. System Ontology

In this system, we propose to use a combination of static and dynamic approaches. Static policy evaluation occurs immediately after negotiation between the producer and consumer, when a filter is applied to the medical record. This simplifies dynamic policy requirements by limiting the data that needs to be evaluated after the bundle is released. If this filter were not applied, the dynamic policy would need to additional clauses to support hiding only those data elements to which the consumer has not been granted access. All other evaluation occurs after the bundle is delivered to the consumer. In order to support more complex and unenvisioned usage scenarios, including evaluating usage based on time constraints, this framework provides extensive dynamic evaluation capabilities after the initial filtering phase. We also need to be able to support seamless operation over protected artifacts while disconnected from any kind of network or communication medium. These factors lead to a powerful *and local* dynamic policy evaluation system.

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-A.pdf.

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

[3] Shifts in Health Information. *New England Journal of Medicine*, 359(2):209–210, 2008.

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

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

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.

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

[16] 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.

[17] 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.

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

[19] 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.

[20] 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.

[21] Kenneth D. Mandl and Isaac S. Kohane. Tectonic Shifts in the Health Information Economy. *New England Journal of Medicine*, 358(16):1732–1737, 2008.

[22] 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.

[23] Jack Powers. Google Health 2018: Best Case Scenarios. http://in3.org/articles/gh2018best.htm, May 2008.

[24] Jack Powers. Google Health 2018: Worst Case Scenarios. http://in3.org/articles/gh2018worst.htm, June 2008.

[25] Jack Powers. Virgin HealthMiles. http://us.virginhealthmiles.com, January 2011.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

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

[31] 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.

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