Tragedy of Anticommons in Digital Right Management of Medical Records

Quanyan Zhu, Carl Gunter and Tamer Başar

Abstract— **The challenge of moving a decentralized, fragmented, paper-based healthcare system to an interconnected, automated, networked world is not merely technological. Digital right management (DRM) technologies can be leveraged as a tool to protect the privacy of electronic health records (EHRs) via encryption, access control, etc. However, the deployment of DRM technology needs to address special requirements for the healthcare system. One of the critical issues is that there is no clearly defined data ownership, and multiple parties own different pieces of a patient's medical history. The fractured ownership of medical information among medical service providers and insurers has created the *tragedy of anticommons* for implementation of DRMs. In this work, we investigate DRM under multiple ownerships of medical data, and employ game-theoretic tools to study and understand the strategic behaviors of different owners in the healthcare system. Our approach aims to address the underutilization of EHR resources, and provides a theoretical basis for mechanism design of economic policies to improve social welfare and efficiency of the electronic healthcare system.**

I. Introduction

The introduction of an interoperable electronic health record (EHR) system can reduce the cost of the healthcare system and enhance the overall quality of treatment by providing healthcare workers timely access to correct and complete information [1]. However, the distribution of healthcare information is still very limited due to concerns about information security and privacy. The misuse of patient's information can result in invasions of privacy and unfair discrimination on the basis of patients' medical histories.

To address the security and privacy concerns of EHRs, digital rights management (DRM) techniques have been proposed to protect personal information of EHRs. DRM is a class of access control technologies that have been widely used by hardware manufacturers, publishers, copyright holders and individuals for protection of intellectual properties of content providers [2]. Information is created by a data owner, and transmitted in a protected form to a recipient via some data distribution channel. The recipient must obtain a license from the right management service (RMS) server. Licenses 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 [3]. The system enables protection of sensitive information from unauthorized use by allowing the data owner to define usage rights and conditions.

Q. Zhu and T. Başar are with Coordinated Science Laboratory and Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, 1308 West Main St., Urbana, IL, 61801, USA. E-mail:{zhu31, basar1}@illinois.edu; C. Gunter is with Department of Computer Science, University of Illinois at Urbana-Champaign, Siebel Center, 201 N. Goodwin, Urbana, IL, USA. E-mail: cgunter@illinois.edu

Although DRM can provide many features desired in a secure electronic healthcare system, the deployment of DRM technology in the healthcare domain is not straightforward. In [2], many special requirements for healthcare DRM system are identified. One of the crucial points discussed is on the data ownership. There is no clearly defined data ownership. In [4], the author points out that the primary barriers are not technological but economic. The economic issues are shaped and driven by basic legal rights in networked medical information. The law's uncertainty over ownership and control of medical information is widely regarded as a major barrier to EHRs.

II. Tragedy of Anticommons

Multiple ownerships of different pieces of a patient's medical history make it difficult for anyone to assemble a complete record. Such socio-economic reality brings difficulties for implementation of DRM. A more precise picture of the DRM model is the one where a recipient needs to obtain information from two data owners who hold different pieces of the record. This makes the application of DRM in the healthcare domain challenging. Each healthcare provider and insurer controls a piece of a patient's complete medical record, and therefore each has the ability to exclude a third party from forming or using the complete record. Since the complete record has greater value than the sum of its parts, there is value to be gained in gathering all the pieces together, but no single provider or insurer has sufficient incentives to accomplish it. This phenomena is an *anticommons problem*, one in which competing rights holders foreclose each other from productive use of a shared resource [5], [6]. Imagine that a user needs to gather patient records from multiple medical facilities. Even though DRM can provide secure access of data from each data owner, the current economic issues in providing patients' EHR access limit the wide deployment and interconnected operations of EHRs. In [7], the authors have listed an array of issues ranging from cost and security concerns to liability issues, from tensions between flexible access to data and flexible access to physicians to patients' limited comprehension of clinical data. All these non-technological issues lead to the reluctance of data access to each medical facility, hence resulting in the anticommons problem.

The anticommons problem was first examined by Michael A. Heller in [6] in regard to disappointing experiences with efforts to shift from socialist to market institutions in Russia. The anticommons problem arises when there exist multiple rights to exclude, and it has become a useful metaphor for understanding how and why potential economic value may disappear into the "black hole" of resource underutilization.

It has been widely used to explain the reason why competing use of copyright can prevent a product from coming to the marketplace at a reasonable price, and why eminent domain or compulsory purchase is considered necessary.

III. Game-Theoretic Approach

We find it essential to use game-theoretic tools to analyze the equilibrium behavior of the anticommons problem in DRM subject to multiple ownerships [8]. We aim to address the underutilization of EHR resources and provide a theoretical basis for mechanism design of economic policies to improve social welfare and efficiency of electronic healthcare systems. Our work is related to the following recent work. In [5], a formal economic model of the anticommons has been proposed. It has been shown that the problems of the commons and the anticommons are symmetrical with algebraic and geometric illustrations. In [9], the authors have established a theoretical model for optimal design of flexible use in a DRM policy, and have shown that the optimal use of flexibility displays an important trade-off between providing a higher value to paying customers and increasing the likelihood of distribution through channels other than legitimate sales.

The game-theoretic model is described by three major components: the players, their action spaces and their utility functions. The players in the context of DRM are medical facilities or data owners of medical records. A single user has to acquire different pieces of medical information from the data owners, and each owner decides on whether or not to provide access to the user. Under the rationality assumption of the players, each owner optimizes his utility function that takes into account important factors such as access cost, security and privacy risks, many of which have been pinpointed in [7].

Nash equilibrium is a fundamental solution concept in non-cooperative game theory. It is an equilibrium outcome of rational decisions where no player can improve by unilaterally deviating from his action. The game-theoretic modeling and analysis facilitate a formal understanding of the efficiency loss as result of noncooperative behaviors in comparison to its cooperative counterpart, where all owners share the data together for access to the public. The mechanism design problem entails the design of a policy through exogenous factors to influence the behaviors of DRM owners. It will allow regulators and government policy makers to modify incentive structures in the current healthcare system. The framework is well aligned with the recent initiative on developing a set of "metadata" standards intended to facilitate exchange of health information [10]. Game-theoretic analysis can help explicate incentives for universal data exchange, and recommend policies to the Health IT Standards Committee and Health IT Policy Committee.

As pointed out in [4], an organizer can pay all necessary providers and insurers to induce their cooperation, but this will raise significant issues under state and federal privacy laws. Even if the issue of ownership is resolved, the existence of multiple stakeholders in a single prize creates strategic behaviors and coordination problems that are difficult to solve through private ordering.

The tragedy of the anticommons explains the lack of interoperability among EHRs. The providers' ownership of medical records is a barrier to EHRs because providers treat patient information as a highly proprietary asset that serves as a means of differentiation from the competition. And as a result, IT vendors compete without data standards and healthcare data becomes institution-based and compartmentalized. Overcoming fractured ownership is critical to constructing a functioning DMR system for EHRs.

IV. Conclusion and Discussions

The disputable issue of the ownership of medical records creates a challenge for direct application of DRM technologies. The primary barriers are not technological but economic. The fractured ownership of medical information among medical service providers and insurers has created the tragedy of commons for implementation of DRMs. Multiple ownerships in DRMs will lead to underutilization of EHR resources even though security and privacy are guaranteed. The problem is critical and needs to be taken into account when designing DRM solutions. We need a simple game-theoretic framework to understand the strategic behaviors of data owners and to be able to analyze the Nash equilibrium of the underlying game. It provides a basis for a deeper understanding of the implementation of DRM technologies as well as a tool for efficient design of incentive mechanisms at the economic level. It is also worth notice that a generalized framework can be developed for a wide class of access management systems in the future.

References

[1] President's Council of Advisors on Science and Technology, "Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward," Dec. 2010.

[2] M. Petković, S. Katzenbeisser and K. Kursawe, "Rights management technologies: A good choice for securing electronic health records?" Intl. Conf. on Information Security Solutions Europe (ISSE), Warsaw, Poland 2007.

[3] N. P. Sheppard, R. Safavi-Naini, and M. Jafari, "A digital rights management model for healthcare," in Proc. of IEEE Intl. Symp. on Policies for Distributed Systems and Networks, 2009.

[4] M. A. Hall, "Property, privacy, and the pursuit of interconnected electronic medical records," Iowa Law Review, no. 95-2, February 2010.

[5] J. M. Buchanan and Y. J. Yoon, "Symmetric tragedies: Commons and anticommons," *Journal of Law and Economics*, vol. 43, no. 1, April 2000, pp. 1-14.

[6] M. A. Heller, "The tragedy of the anticommons: property in the transition from Marx to markets," 111 *Harvard Law Review*, pp. 621–688 , 1998.

[7] L. Beard, R. Schein, D. Morra, K. Wilson and J. Keelan, "The challenges in making electronic health records accessible to patients," *Journal of the American Medical Informatics Association*, 2011.

[8] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, SIAM Series in Classics in Applied Mathematics, January 1999.

[9] D. Bergemann, T. Eisenbach, J. Feigenbaum, and S. Shenker, "Flexibility as an Instrument in DRM Systems," 2005 Workshop on Economics of Information Security.

[10] Department of Health and Human Services, Office of the Secretary,"Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology," 45 CFR Part 170, RIN 0991-AB82.