An Ontology for a HIPAA compliant cloud services

Karuna Pande Joshi, Yelena Yesha and Tim Finin
Computer Science and Electrical Engineering
University of Maryland, Baltimore County
{karuna.joshi, yelena.yesha, finin}@umbc.edu

Introduction

With increasing adoption of digitized patient records and physician's notes, managing patient records and medical data has become a major challenge for healthcare providers. Hence, cloud based healthcare services have flooded the market with their promise of ubiquitous access, scalability and low cost. The Health Insurance Portability and Accountability Act (HIPAA) [1] regulates the privacy and security of this data maintained by the healthcare providers and all cloud based healthcare services in the United States must comply with it. The HIPAA Privacy Rule [3] protects the privacy of individually identifiable health information, called protected health information (PHI). The Security Rule [4] protects a subset of information covered by the Privacy Rule, which includes all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form.

We have developed a semantically rich Web Ontology Language (OWL) ontology to define the HIPAA privacy and security rules. This ontology extends the service lifecycle ontology that we have developed for automatically acquiring and consuming cloud based services [2] in that it helps define healthcare domain specific security and privacy measures. Our HIPAA ontology defines in detail the concepts that have been specified in the act. Using this ontology in conjunction with our Cloud lifecycle ontology and incorporating the compliance and security guidelines in [5], users can discover and acquire Healthcare services that will comply with HIPAA security requirements. In this paper we describe this ontology in detail. Organizations consuming or migrating to cloud based Electronic Medical Records (EMRs) can use this ontology to determine the security and privacy policies that should be implemented by the cloud service provider in order to ensure HIPAA compliance.

HIPAA Domain Ontology

We model the ontology into three main components – stakeholders, security rules and privacy rules.

Key Stakeholder classes

The main classes of stakeholders include covered entities, business associates, exempt entities and patients (see figure 1). The covered entities comprises of subclasses of health care providers, health plans and clearing houses. The main healthcare provider classes are Doctors, Clinics, Hospitals, Pharmacies, Dentists, Psychologists and Nursing homes. These are all covered by the HIPAA security and privacy rules. The business associates are entities that have a contract/sub-contract with the healthcare providers to provide one or more services related to healthcare. As a result of this contract, the business associates have access to the PIH data and are thus covered by the HIPAA rules. In addition to the two main classes, we have a class of Exempt entities who are exempt from HIPAA rules even though they may collect personal health data. The main sub-classes under exempt entities are Schools, Employers, State agencies, Life Insurer, Law enforcement agencies, worker compensation carrier and municipal offices.

Security Rules classes

The HIPAA security rules are applicable to the covered entities and business associates who transmit patients' health information in electronic form in connection with a transaction. The main classes, illustrated in Figure 1, are security rules, safeguards, risk analysis and personal health information (includes diagnosis,

treatment and doctor conversations). Safeguards class is further divided into administrative, physical and technical safeguards that are detailed in figure 1.

Privacy Rules classes

The HIPAA privacy rules are applicable to the covered entities and business associates who transmit patients' health information in electronic form in connection with a transaction. The main classes (illustrated in Figure 1) are 'permitted use or disclosure' which includes scenarios in which the covered entities can share the PHI, 'authorized use or disclosure' that includes situations where the covered entities can share PHI after authorization by patients and administrative requirements of maintaining privacy.

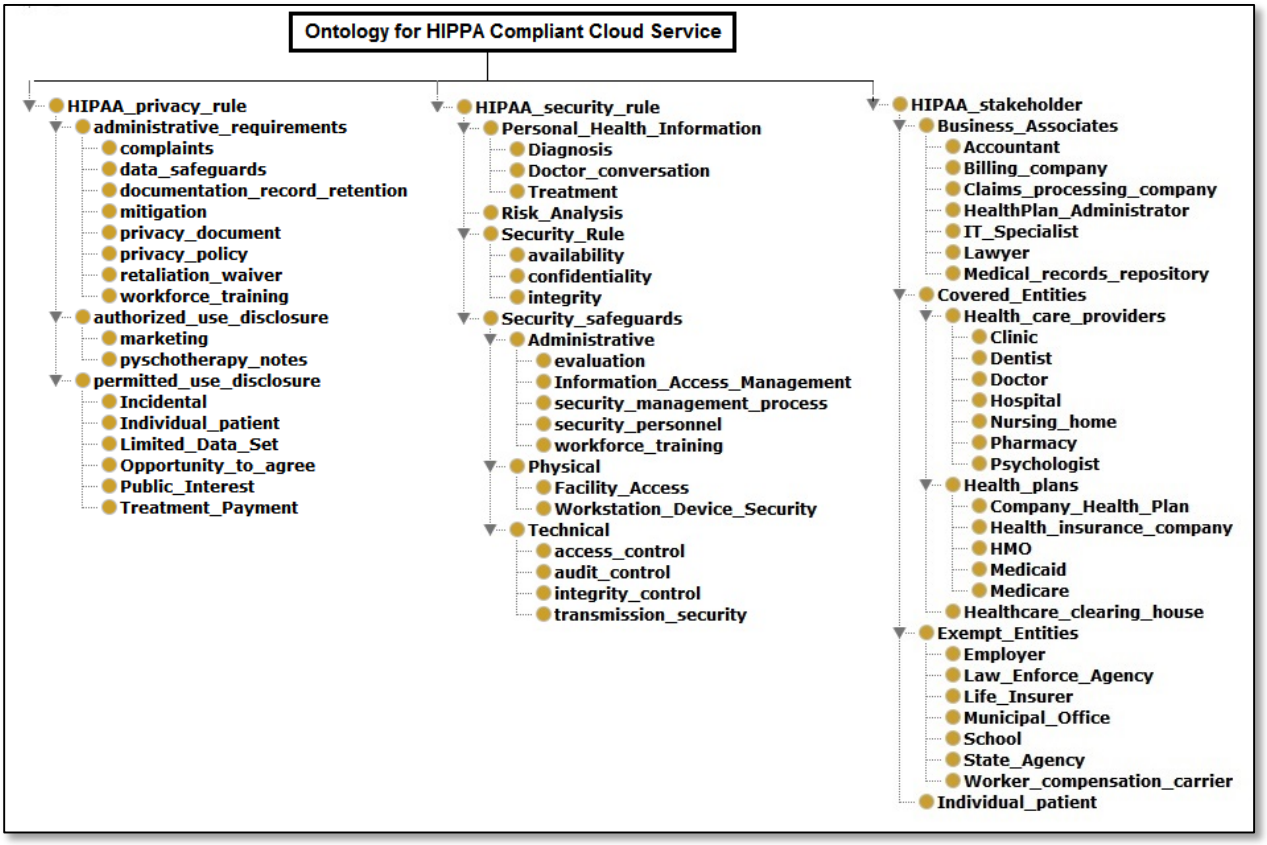

Figure 1: Key Stakeholders in the HIPAA ontology

References

[1] Joshi, K.P.; Yesha, Y.; Finin, T., Automating Cloud Services Lifecycle through Semantic Technologies, IEEE Transactions on Service Computing, vol.7, no.1, pp.109-122, Jan.-March 2014

[2] Health Information Privacy, http://www.hhs.gov

[3] Centers for Disease Control and Prevention. "HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services." *MMWR: Morbidity and Mortality Weekly Report* 52.Suppl. 1 (2003): 1-17.

[4] Hash, Joan. *An introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule*. Diss. National Institute of Standards and Technology, 2005.

[5] A. Hendre and K. P. Joshi, "A Semantic Approach to Cloud Security and Compliance," 2015 IEEE 8th International Conference on Cloud Computing, New York City, NY, 2015, pp. 1081-1084.